

webMethods Mobile Administrator User's Guide

Version 9.9

October 2015

This document applies to webMethods Mobile Administrator Version 9.9 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Copyright © 2014-2015 Software AG, Darmstadt, Germany and/or Software AG USA Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA Inc. and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <http://softwareag.com/licenses>.

Use of this software is subject to adherence to Software AG's licensing conditions and terms. These terms are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software AG Products / Copyright and Trademark Notices of Software AG Products". These documents are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

Use, reproduction, transfer, publication or disclosure is prohibited except as specifically provided for in your License Agreement with Software AG.

Table of Contents

About This Guide	11
Document Conventions.....	11
Online Information.....	12
Getting Started with Mobile Administrator	13
What is Mobile Administrator?.....	14
Installation and Prerequisites.....	14
Invoking Mobile Administrator.....	15
First Steps After the First Login.....	16
Checking the User Profile.....	17
Overview of Permissions.....	18
The Mobile Administrator User Interface.....	19
Viewing Information on the App Store Client.....	21
Simulating a Mobile Device.....	21
Filtering Lists.....	22
Exporting Lists to Excel Format.....	22
Uploading Files.....	23
The Dashboard.....	23
Resetting Your Password.....	24
Logging Out.....	25
Configuring Mobile Administrator	27
Overview.....	28
Using the Configuration Assistant.....	28
Adding the Mobile Administrator License File.....	30
Specifying the Domain Details.....	30
Adding Users.....	31
Adding Local Users.....	31
Connecting to an LDAP Server.....	31
Granting Site-Level Permissions to a User.....	32
Adding Code Signing Certificates for iOS.....	32
Generating and Uploading an iOS Distribution Certificate.....	33
Uploading an iOS Provisioning Profile.....	33
Adding Code Signing Certificates for Android.....	34
Uploading a Developer Certificate for Android.....	34
Adding Code Signing Certificates for Windows Phone.....	34
Uploading the Windows Phone 8 Application Enrollment Token.....	34
Uploading a Developer Certificate for Windows Phone.....	35
Adding Code Signing Certificates for Windows 8/RT.....	35
Uploading a Developer Certificate for Windows 8/RT.....	35
Connecting Build Nodes.....	36

Connecting a Build Node for iOS and Android.....	36
Connecting a Build Node for Windows Phone and RT.....	38
Creating and Launching Build Configurations for the App Store Client.....	41
Creating the Build Configuration for the iOS Platform.....	41
Verifying the Bundle ID for the App Store Client.....	41
Creating the iOS Build Configuration for the App Store Client.....	42
Creating the Build Configuration for the Android Platform.....	42
Creating the Build Configuration for the Windows Phone Platform.....	42
Creating the Build Configuration for the Windows 8/RT Platform.....	43
Launching the Build Configurations for the App Store Client.....	43
Configuring the Mobile Device Management.....	44
Uploading an MDM Certificate for iOS.....	45
Specifying a GCM API Key for Android.....	45
Managing Apps.....	47
Overview.....	48
The All Applications Page.....	49
Organizing Apps in Categories.....	50
Adding a Category.....	50
Editing a Category.....	52
Deleting a Category.....	52
Adding an App.....	53
Adding an Application Binary.....	56
Importing an App.....	56
Adding an App from a Vendor App Store.....	57
Adding an App from Another Mobile Administrator Instance.....	57
Specifying the Details for the New App Manually.....	58
Displaying an App.....	61
Managing the App Details.....	63
Editing an App.....	65
Batch-Editing Several Apps.....	65
Sharing an App.....	66
Exporting an App.....	66
Viewing the Log Information for an App.....	67
Deleting an App.....	67
Managing the Versions of an App.....	68
Adding a New App Version.....	69
Editing an App Version.....	70
Making an App Version Stable.....	70
Attaching an Executable to an App Version.....	71
Adding a New App Version from an Executable.....	72
Downloading an Executable.....	72
Deleting an Executable.....	73
Displaying the Release Notes for an App Version.....	73
Displaying the Build Jobs for an App Version.....	74

Displaying the Crash Logs for an App Version.....	74
Displaying the Comments for an App Version.....	75
Deleting an App Version.....	76
Managing the Resources of an App.....	76
Adding a New Resource Manifest.....	77
Adding Resource Files to a Manifest.....	78
Deleting Resource Files from a Manifest.....	78
Finalizing a Resource Manifest.....	79
Duplicating a Resource Manifest.....	79
Changing the Availability Date of a Resource Manifest.....	80
Changing the Bundled Status of a Resource File.....	80
Downloading a Single Resource File.....	81
Downloading a Resource Manifest as a Human-Readable Zip File.....	81
Downloading a Resource Manifest as a Bundle Zip File.....	82
Downloading the Finalized Manifest as a Binary Large Object.....	82
Deleting a Resource Manifest.....	82
Managing the Permissions of an App.....	83
Overview of Application-Level Permissions.....	84
Granting Application-Level Permissions to a User or User Group.....	85
Editing the Application-Level Permissions of a User or User Group.....	85
Removing the Application-Level Permissions of a User or User Group.....	86
Managing the Builds of an App.....	86
Managing the Build Configurations of an App.....	87
Overview of App Policies.....	88
Adding a Build Configuration.....	91
Launching a Build Configuration.....	95
Editing a Build Configuration.....	96
Duplicating a Build Configuration.....	96
Removing a Build Configuration.....	96
Managing the Build Jobs of an App.....	97
Managing the Source Code Repositories of an App.....	97
Adding a Source Code Repository.....	98
Editing a Source Code Repository.....	99
Removing a Source Code Repository.....	99
Managing the Devices on Which the App Can be Installed.....	100
Installing an App on a Managed Device.....	101
Updating an App on a Managed Device.....	101
Removing an App from a Managed Device.....	101
Managing the Push Notifications for an App.....	102
Adding Certificates for the Apple Push Notification Service (APNS).....	103
Specifying an API Key for Google Cloud Messaging (GCM).....	104
Sending a Push Notification.....	104
Using the Apple App Store Volume Purchase Program (VPP).....	104
Adding a Single Redemption Code.....	105
Importing Multiple Redemption Codes.....	106

Deleting a Redemption Code.....	106
Viewing the App Analytics.....	107
Managing Devices.....	109
Overview.....	110
The All Devices Page.....	110
Organizing Devices in Groups.....	111
Adding a User Group as a Device Group.....	111
Adding a Device Group.....	112
Adding a Policy to a Group.....	112
Removing a Policy from a Group.....	113
Adding a Device to a Device Group.....	113
Removing a Device from a Device Group.....	113
Deleting a Device Group.....	114
Managing a Device.....	114
Adding Policies to a Device.....	116
Removing Policies from a Device.....	116
Remotely Locking a Device.....	117
Updating the Device Information.....	117
Remotely Wiping a Device.....	118
Pinging a Device.....	118
Viewing the Commands that have been Sent to a Device.....	118
Removing the Mobile Device Management (MDM) from a Device.....	119
Removing a Device.....	120
Managing Policies.....	121
Overview.....	122
The All Policies Page.....	122
Adding a Device Policy.....	123
Viewing the Policy Details.....	123
Editing a Device Policy.....	124
Deleting a Device Policy.....	124
Policy Types.....	125
Exchange Account Policy.....	125
Home Button Policy.....	125
Passcode Policy.....	126
Restrictions Policy.....	126
VPN Service Policy.....	128
Web Clip Policy.....	129
WiFi Network Policy.....	129
Managing Domains.....	131
Overview.....	132
The All Domains Page.....	132
Viewing the Domain Details.....	132
Editing the Domain.....	133

Allowing Access for Users from an LDAP Directory.....	135
Creating a New Domain.....	136
Checking the Space Usage.....	137
Viewing the MDM Certificates.....	137
Deleting a Domain.....	138
Managing Users.....	139
Overview.....	140
The All Users Page.....	140
Overview of Site-Level Permissions.....	141
Adding a Local User.....	142
Managing the User Details.....	143
Changing the Avatar for a User.....	144
Editing the User Details.....	145
Specifying the Notifications that a User Receives.....	146
Adding an Access Token for a User.....	146
Deleting an Access Token for a User.....	147
Adding a User to a Local User Group.....	148
Removing a User from a Local User Group.....	148
Deleting a User.....	149
Managing User Groups.....	151
Overview.....	152
The All User Groups Page.....	152
Creating a Local User Group.....	152
Viewing the Members of a User Group.....	153
Changing the Name of a Local User Group.....	153
Deleting a User Group.....	153
Managing Build Nodes.....	155
Overview.....	156
The All Build Nodes Page.....	156
Adding a Build Node.....	158
Deleting a Build Node.....	158
Managing Build Jobs.....	159
Overview.....	160
The All Build Jobs Page.....	160
Displaying the Details of a Build Job.....	161
Running Tests.....	162
Scheduling a Build Job.....	162
Relaunching a Build Job.....	162
Showing the Console Output for a Build Job.....	163
Showing the Errors for a Build Job.....	164
Deleting a Build Job.....	164

Managing Product Stages.....	167
Overview.....	168
The All Product Stages Page.....	168
Adding a Product Stage.....	168
Deleting a Product Stage.....	169
Managing Developer Certificates.....	171
Overview.....	172
The All Certificates Page.....	172
Deleting a Certificate.....	173
Managing Provisioning Profiles.....	175
Overview.....	176
The All iOS Provisioning Profiles Page.....	176
Deleting a Provisioning Profile.....	176
Re-Signing Applications.....	179
Overview.....	180
The Application Re-sign Page.....	180
Re-signing an iOS App.....	181
Re-signing an Android App.....	181
Re-signing a Windows Phone App.....	182
Re-signing a Windows 8/RT App.....	182
Deleting a Re-signing Job.....	183
Sales and Trends on iTunes Connect.....	185
Overview.....	186
The All iTunes Connect Vendors Page.....	186
Adding a New iTunes Connect Vendor.....	186
Editing the Vendor Information.....	187
Downloading Reports From iTunes Connect Manually.....	187
Adding Reports to Mobile Administrator Manually.....	187
Exporting Reports to Your File System.....	188
Deleting All Reports.....	188
Deleting a Vendor.....	188
Maintaining Mobile Administrator.....	189
Overview.....	190
The Maintenance Page.....	190
Domain Log.....	190
Server Logs.....	191
Cleanup Tasks.....	191
Process Info.....	192
Using the App Store on a Mobile Device.....	193
Overview.....	194

Using the App Store Client on a Mobile Device.....	194
Installing the App Store Client.....	194
Using the App Store Client.....	195
Allowing the Mobile Device Management.....	197
Remotely Locking or Wiping a Mobile Device.....	197
Removing the Mobile Device Management.....	198
Using the App Store Website on a Mobile Device.....	199
Accessing the App Store in the Browser.....	199
Using the App Store in the Browser.....	199
Frequently-Asked Questions.....	201
App Management.....	202
Device Management.....	202
Certificate Management.....	203

About This Guide

This guide explains how to configure and use webMethods Mobile Administrator and its build environment for mobile applications. It explains how to set up an app store from which your end users (for example, employees or customers) can download onto their mobile devices the apps that you have developed yourself or apps from other vendor stores that you have made available for download in your own app store.

The information in this guide is intended for administrators and developers who want to build mobile applications and manage mobile devices for iOS, Android and Windows platforms. End users, who usually only have the right to download apps, will also find useful information on how to access the app store and manage their own devices.

If you want to access Mobile Administrator through the REST API, see the *webMethods Mobile Administrator API Reference*.

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
Narrowfont	Identifies storage locations for services on webMethods Integration Server, using the convention <i>folder.subfolder:service</i> .
UPPERCASE	Identifies keyboard keys. Keys you must press simultaneously are joined with a plus sign (+).
<i>Italic</i>	Identifies variables for which you must supply values specific to your own situation or environment. Identifies new terms the first time they occur in the text.
Monospace font	Identifies text you must type or messages displayed by the system.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the symbol.

Convention	Description
[]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Online Information

Software AG Documentation Website

You can find documentation on the Software AG Documentation website at <http://documentation.softwareag.com>. The site requires Empower credentials. If you do not have Empower credentials, you must use the TECHcommunity website.

Software AG Empower Product Support Website

You can find product information on the Software AG Empower Product Support website at <https://empower.softwareag.com>.

To submit feature/enhancement requests, get information about product availability, and download products, go to [Products](#).

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the [Knowledge Center](#).

Software AG TECHcommunity

You can find documentation and other technical information on the Software AG TECHcommunity website at <http://techcommunity.softwareag.com>. You can:

- Access product documentation, if you have TECHcommunity credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

1 Getting Started with Mobile Administrator

■ What is Mobile Administrator?	14
■ Installation and Prerequisites	14
■ Invoking Mobile Administrator	15
■ First Steps After the First Login	16
■ Checking the User Profile	17
■ Overview of Permissions	18
■ The Mobile Administrator User Interface	19
■ Viewing Information on the App Store Client	21
■ Simulating a Mobile Device	21
■ Filtering Lists	22
■ Exporting Lists to Excel Format	22
■ Uploading Files	23
■ The Dashboard	23
■ Resetting Your Password	24
■ Logging Out	25

What is Mobile Administrator?

Mobile Administrator is used to set up an enterprise app store that enables you to quickly distribute apps and updates to the mobile devices of your employees or customers.

You can deploy and manage apps, and you can manage mobile devices. Mobile Administrator supports the concepts of "bring your own device" (BYOD) and "choose your own device" (CYOD).

You can set up and configure remote build nodes. Your builds can thus run in the cloud without developers having to run build environments for all platforms on their developer devices.

It is possible to enforce app policies. This enables the same mobile device for both private and business usage without compromising confidential data of your enterprise.

Apps can remotely be removed from the mobile devices, for example, if employees leave your company. Mobile devices can be locked or wiped, for example, if these devices are lost or stolen.

Mobile Administrator provides runtime statistics and allows you to monitor the usage of your apps. If an app crashes, the corresponding crash reports and system logs are automatically collected and analyzed.

Mobile Administrator manages your enterprise certificates and the platform development programs with their specific usage terms. Mobile Administrator can notify you if certificates expire.

Mobile Administrator uses token-based authorization for its components (such as apps and build nodes). Each component asks the user to enter the user name and password in order to obtain a token. This token allows the component to access a specific resource without using the user name and password.

Installation and Prerequisites

Mobile Administrator is installed using the Software AG Installer. See *Using the Software AG Installer* and *Installing Software AG Products* for detailed information.

Supported Server Platforms and Browsers

The server component of Mobile Administrator can be installed on Linux. The user interface of Mobile Administrator runs in a browser. For detailed information on the supported operating system platforms and browsers, see *System Requirements for Software AG Products* on the Software AG Documentation website at <http://documentation.softwareag.com/> (Empower login required).

Supported Build Nodes

webMethods Mobile Designer must be installed on the machine on which you want to set up the build node. For information on how to set up Mobile Designer, the required SDKs and other required software, see *Using webMethods Mobile Designer*.

Mobile Administrator supports build nodes on:

- **Mac OS X (Version 10.7 or later).** This build node uses the iOS SDK and the Android SDK to build mobile apps and upload the results to the server.
- **Windows 8 Pro.** This build node uses the Windows Phone SDK and the Windows SDK to build mobile apps and upload the results to the server.

Supported Mobile Platforms and File Formats

Mobile Administrator supports the following platforms and file formats:

Platform	File Format
iOS	.ipa
Android	.apk
Windows 8, Windows RT, Windows Phone as of version 8.1	.appx and .appxupload
Windows Phone 8.0 and below	.xap

Invoking Mobile Administrator

When you log in to Mobile Administrator for the first time after it has been installed, you have to use the default user name "admin" and the default password "admin".

Note: To avoid security problems, you should change this default password right after your first login.

For instructions how to change the password, see ["Checking the User Profile" on page 17](#).

By default, all possible permissions are granted to this user. The "admin" user can change all aspects of Mobile Administrator and is responsible for configuring Mobile Administrator (for example, to define the users and configure the build environment).

Note: This documentation is intended for administrators, that is, for users to whom all possible permissions have been granted. If you only have limited

permissions, many functions described in this documentation are hidden to you.

When Mobile Administrator has been configured, all defined users can access Mobile Administrator. These can either be the users defined in an LDAP system (these users log in with the user name and password credentials stored for them in the LDAP) or users that have manually been defined in Mobile Administrator (these users log in with the user name and password credentials stored for them in Mobile Administrator).

If the licensed number of active users is reached, additional users cannot log in. However, users with the site-level permission **Manage Site** can always log in, regardless of the licensed number of users. For more information on the license limits, see "[Adding the Mobile Administrator License File](#)" on page 30.

Note: The logo that is shown on the login page can be changed by editing the domain details. See "[Editing the Domain](#)" on page 133.

To invoke Mobile Administrator

1. Invoke your browser and enter the URL for invoking Mobile Administrator.

If you are the administrator and you want to invoke Mobile Administrator for the first time directly after the installation, Mobile Administrator will be available via HTTP or HTTPS at the IP address of the host machine.


After the administrator has configured Mobile Administrator as described in "[Specifying the Domain Details](#)" on page 30, all users can invoke Mobile Administrator by entering the URL that they have received from the administrator.
2. On the resulting login page, enter your user name and password.
3. Optional. If you want to invoke Mobile Administrator directly, without having to log in each time, make sure that **Keep me logged in** is selected. When this check box is not selected, you are automatically logged out when you close the browser window.
4. Click **Log in**.

First Steps After the First Login

When the default user with the name "admin" logs in to Mobile Administrator for the very first time, a **setup your site** link is shown in a message box at the top of the page. Using this link, the administrator can invoke the Configuration Assistant. Before other users can work with Mobile Administrator, the administrator has to complete several configuration steps which include the definition of users and the configuration of the build environment.

As long as Mobile Administrator has not been configured, the **setup your site** link is shown on each Mobile Administrator page.

To set up Mobile Administrator

1. Click the **setup your site** link. Set up your site as described in "[Configuring Mobile Administrator](#)" on page 27.
 2. After you have configured Mobile Administrator, it is recommended that you make sure that unauthorized users will not be able to log in with administrator permissions. Therefore, click  and then **User Profile**. Proceed as follows:
 - a. Rename the default user "admin".
 - b. Define a new password.
 - c. Define your email address so that you can receive emails, for example, when you need to reset your password or when Mobile Administrator sends out notifications.
- Note:** By default, the email address admin@admin.com is defined for the administrator. This is a fake address. Make sure to change this to an existing email address.
- d. Keep all permissions as they are.
 3. Add a second administrator user - just in case - with all possible site-level permissions.

Checking the User Profile

What you can see and change in Mobile Administrator depends on the permissions that have been granted to you. You can check your user profile to find out which permissions you have. These are the so-called site-level permissions (see also "[Overview of Permissions](#)" on page 18). You need appropriate permissions to be able to manage devices or apps. If your user profile does not show any permissions, you are a normal user with the right to view and download apps from the app store. Site-level permissions are usually only assigned to a user who is to act as an administrator.

The user profile shows the following information for all users:

- The image (avatar) that is to be shown for the user. Each user can change the own avatar.

Note: If the user's email address is registered at gravator.com, this service will be used to show the "Globally Recognized Avatar", unless the user uploads an image with Mobile Administrator.

- User name and email address.
- The apps that are assigned to the user. This assignment is done automatically when a user adds an app. Each user can click an app to display information about it.

- The access tokens that have been generated by this user account. Access tokens are generated for the components (such as apps or build nodes) and are needed for authentication in Mobile Administrator.

A user with administrator permissions can see and change more information. An administrator is able, for example, to change the site-level permissions.

The following command buttons are available in the user profiles of all users:

Button	Description
Edit User	Each user can change the password and email address. A user with the site-level permission Manage Users and Groups can also change first name and last name, and the permissions.
Notifications	For a normal user with no site-level permissions, the apps assigned to that user are shown. If the user has the site-level permission Manage Apps , all currently defined apps are shown. Each user can specify whether to receive an email when an app gets an update or when someone comments on an app.

When a user has the site-level permission **Manage Users and Groups**, a **Delete User** button is also available in the user profile. When you delete yourself, you will be logged out automatically. However, if you are the only user with administrator permissions in this instance of Mobile Administrator, you will not be able to delete your user profile. See also "[Managing the User Details](#)" on page 143.

To access the user profile

- Click  and then **User Profile**.

Overview of Permissions

Mobile Administrator distinguishes two types of permissions:

- **Site-level permissions.** These permissions are granted to users. For example, they can allow a user to add and manage apps or to remotely wipe managed devices. Only a user with the site-level permission **Manage Admin Permissions** is able to define/restrict the permissions for other users. See also "[Overview of Site-Level Permissions](#)" on page 141.
- **Application-level permissions.** These permissions are defined individually for single apps. They can be granted to users and user groups. As a rule, all users have the permission to download stable versions of an app. But it is also possible to allow one or more users, for example, to change the metadata of an app (this includes the icon and description), to add or remove versions of an app, or to trigger the removal of an

app on managed devices. See also "[Overview of Application-Level Permissions](#)" on [page 84](#).

Note: In addition to the above mentioned permissions, it is also possible to define policies for an app. For example, you can disable copy and paste within the app, force authentication before the app can be used, or define an expiration date for the app. For more information, see "[Overview of App Policies](#)" on [page 88](#).

The Mobile Administrator User Interface

Depending on the granted permissions, users can either manage different aspects of Mobile Administrator (such as apps, policies and devices) or just download apps from the app store. There are different views for administrators and normal users.

When a user with administrator permissions logs in to Mobile Administrator, the pages listed below are available. You invoke a page by clicking on the corresponding image in the navigation bar, which is shown at the top of the page.














Image	Description
	<p>This is the home button. Depending on the user's permissions, the home button shows either the dashboard (administrator) or the app store (normal user). By default, a Software AG logo is shown on the home button.</p> <p>Note: The logo for the home button can be changed by editing the domain details. See "Editing the Domain" on page 133.</p>
 App Store	<p>Shows the contents of your app store. The latest stable app versions are shown. You can click an app to view it as it would appear in your app store.</p>
 Manage Apps	<p>Used to add and manage apps, and to define how they appear in the app store. See "Managing Apps" on page 47.</p>
 Devices	<p>Shows all devices on which your app store client has been installed and the users who own these devices. You can add user groups and device groups with different policies. See "Managing Devices" on page 109.</p>

Image	Description
 Policies	Shows all defined policies. You can edit or delete the existing policies, and you can add new policies. See " Managing Policies " on page 121.
 Dashboard	Shows the dashboard which provides several information boxes. You can see, for example, which app has last been created or changed. See " The Dashboard " on page 23.

Note: A normal user can only see the home button and the  [App Store](#) and  [Devices](#) links, where the latter only allows to manage the user's own devices. When the user has allowed the device management on the mobile device, this user can, for example, lock or wipe the own device. The corresponding site-level permissions are not required in this case.

In addition, the following icons are shown at the top right of the page:

Icon	Description
	Allows you to access the Mobile Administrator documentation on the Software AG documentation website (Empower login required).
	Shows the so-called "settings" menu. Using the commands in this menu, you can manage different aspects of Mobile Administrator. For example, you can define all required settings for your domain, or you can manage the user groups. See the corresponding sections later in this documentation for detailed information on each command.
	Shows the so-called "user" menu. Using the commands in this menu, you can manage your user profile and the app that is to be used as your app store client. You can browse an app as it would be shown in a specific device (for example, with a specific Android model), and you can log out from Mobile Administrator. See the corresponding sections later in this documentation for detailed information on each command.

Note: A normal user can only see the  and  icons.

Viewing Information on the App Store Client

The users can download apps onto their mobile devices either directly from a web page in the browser or by using a special app, the so-called app store client. See also "[Using the App Store on a Mobile Device](#)" on page 193.


Before the users can download and install the app store client, an administrator first has to build the app store client for each mobile platform on which it is to be made available. For detailed information, see "[Creating and Launching Build Configurations for the App Store Client](#)" on page 41.

When a user views the information on the app store client from within Mobile Administrator, the shown information depends on the user permissions:

- A normal user can only see a screen with similar information as shown for any other app in the app store (such as version number, platforms, description, screenshots, comments).
- A user with the site-level permission **Manage Apps** can see a screen on which all aspects of the app can be managed. For example, this user can specify a different name or icon for the app store client, or can enter a individual description and contact information. See also "[Managing Apps](#)" on page 47.

Caution: If you delete the app store client using the **Delete** button, all of your app store versions for all platforms are deleted. To restore your app store client in such a case, you have to rebuild it.


To view information on the app store client

- Click  and then **App Store Client**.

Simulating a Mobile Device

You can simulate browsing with different mobile devices. Mobile Administrator will then only show the apps which are able to run on that device. For example, you can select a Nexus device (Android) if you want to see which of your apps can run on this device.

To simulate a mobile device

1. Click  and then **Browse as**.
2. Select a model from the list.
3. Click **Submit**.

A red box with the text "App Store as seen by *device-name*" is now shown at the bottom of the **App Store** and **All Applications** pages. As long as you do not click the **Reset 'Browse as'** link in the red box, these pages only show the apps that are able

to run on the selected device. The red box is not shown on other pages as this functionality has no relevance there.

Filtering Lists

Many pages which show a list of items allow you to define a filter so that you can immediately find the information in which you are interested. When this is possible, a **Filter** box is shown above the list. The characters that you type in may be contained in any column of the list and at any position within an entry or word. The filter criteria are not case-sensitive.

Keep in mind that your filter will also find elements that are not shown in the list but are, for example, part of a link. For example, when you enter a single letter such as "b" on the **All Devices** page, the list may not change much. When you move the mouse over an entry to show the URL at the bottom of your browser window, however, you will see that letter. Therefore, always try to enter as much characters as possible when defining your filter.

With the appropriate filter, you can display, for example:

- On the **All Applications** page in list view (☰): only the apps that contain the string "demo" in the app name.
- On the **All Devices** page: only the entries for a specific phone model or Android version.
- On the **All Users** page: only the users that have been seen on a specific date or who have "never" been seen.

To filter a list

1. Display a page which shows a list of items. For example:
 - Click ☰ **Manage Apps** and go to the list view (☰).
 - Or click 📱 **Devices**.
2. Type your filter in the **Filter** box.





The list changes with each character that you type in. You need not press ENTER.

Exporting Lists to Excel Format

Many pages which show a list of items allow you to export the entire list to Excel (XLS) format. When this is possible, a ▼ menu containing the command **Export (XLS)** is shown on the page. Filters that are currently defined for a list are ignored in the exported result.

To export a list to Excel format

1. Display a page which shows a list of items. For example:

- Click  **Manage Apps** and go to the list view (.
 - Or click  **Devices**.
2. Click  and then **Export (XLS)**.

Depending on your browser and the platform on which you are currently using Mobile Administrator, the information will either be downloaded immediately, or you may be asked whether you want to open or save it.


Uploading Files

Many pages provide one or more **Browse** buttons which allow you to upload files from the file system. You can either use a dialog box to select the file to be uploaded or you can use drag-and-drop.

To upload a file

1. Display a page which provides a **Browse** button.
2. Do one of the following:
 - Click **Browse** and then select the file to be uploaded from the resulting dialog box.
 - Drag the file from the file system and drop it on the appropriate **Browse** button.

The Dashboard

If you have the site-level permission **Manage Site** you can access the dashboard by clicking  **Dashboard** or the domain logo (home button) which is shown at the very left of the navigation bar.

The dashboard provides the following information boxes:

Information Box	Description
Activity Stream	Shows an overview of the last 50 events. This includes the creation and modification of an app or app version, user comments and app ratings. Links are provided so that you can immediately go to the corresponding app or app version. You can also click the header of this information box to display the events from this box on a separate Activity Stream page.
Recent App Updates	Shows the last 5 apps which have been updated. You can click an app to display it. You can also click the header of this information box to display

Information Box	Description
	the All Applications page. See also " Managing Apps " on page 47.
Weekly App Downloads	Shows a graph which indicates the number of apps that have been downloaded in the last 7 days.
Top Downloads This Week	Shows the most popular apps which have been downloaded in the last 7 days. You can click an app to display it. You can also click the header of this information box to display the All Applications page. See also " Managing Apps " on page 47.
Managed Devices	Shows a pie chart which indicates the proportional distribution of the managed devices over the supported platforms. These are the devices which have been registered in Mobile Administrator and on which the mobile device management (MDM) has been allowed. You can click the header of this information box to display the All Devices page which lists all devices, no matter whether MDM has been allowed or not. See also " Managing Devices " on page 109.
Domain Information	Shows the number of active users, managed devices, apps, build nodes, today's build jobs and the current disk usage. You can click on a number to display more information. For example, when you click on the user number, the All Users page is shown which lists the user names. Expiration information for your Mobile Administrator license is also shown. A regular license does not have an expiration date; "never" is shown in this case. An expiration date will be shown, however, if you are using test license which is only valid for a certain period of time.

Resetting Your Password

If you have forgotten your password, you can request a new one. It will then be sent to the email address that you specify. Make sure to specify the same email address as defined in your user profile.


To reset the password

1. Invoke your browser and enter the URL which invokes Mobile Administrator.
2. On the login page, click **Forgot your password?**
3. On the resulting page, enter your email address and click **Reset Password**.
4. Check your email. A link in the email will direct you to a page on which you can set a new password.

Logging Out

When the option **Keep me logged in** is selected during the login, you are automatically logged in each time you enter the URL for invoking Mobile Administrator. If you want to log in as a different user, you have to log out first.

To log out

- Click  and then **Logout**.

2 Configuring Mobile Administrator

■ Overview	28
■ Using the Configuration Assistant	28
■ Adding the Mobile Administrator License File	30
■ Specifying the Domain Details	30
■ Adding Users	31
■ Adding Code Signing Certificates for iOS	32
■ Adding Code Signing Certificates for Android	34
■ Adding Code Signing Certificates for Windows Phone	34
■ Adding Code Signing Certificates for Windows 8/RT	35
■ Connecting Build Nodes	36
■ Creating and Launching Build Configurations for the App Store Client	41
■ Configuring the Mobile Device Management	44

Overview

This chapter explains how to configure a domain in Mobile Administrator. You should do this directly after the installation, when accessing Mobile Administrator for the very first time. One Mobile Administrator instance can host multiple domains. To use Mobile Administrator, you need to set up at least one domain. Mobile Administrator comes with a default domain, where "default" is defined as the domain name.

Make sure to access Mobile Administrator with full administrator rights. The default user, who has the following credentials, has these rights:

- User name: admin
- Password: admin

Note: This chapter just briefly explains the functions that are required to set up Mobile Administrator. For more detailed information on these functions and the options that can be specified, see the corresponding chapters later in this guide.

Using the Configuration Assistant

It is recommended that you configure Mobile Administrator using the Configuration Assistant. The Configuration Assistant lets you comfortably access the pages on which you have to specify the required information to get started. It allows you to:

- Add the license file.
- Add users (local users or users from an LDAP system).
- Upload code signing certificates for the platforms on which you want to make available your apps (iOS, Android and Windows Phone).
- Connect to a build node on Mac OS X or Windows 8.
- Create the build configurations for iOS, Android and Windows Phone platforms.
- Build the app store clients for iOS, Android and Windows Phone platforms.
- Configure mobile device management (MDM) for iOS and Android.

Note: Mobile device management is not yet supported on Windows Phone platforms.

Depending on the features and mobile platforms that you want to use with Mobile Administrator, you need not complete all configuration steps. The Configuration Assistant provides a drop-down list box from which you can select a platform (for example, iOS or Android). The configuration page will then only show the steps that are

required for the selected platform. When a configuration step has been completed, the Configuration Assistant displays a check mark for this step.

Configuration Assistant

Platform

Domain

Add webMethods Mobile Administrator License to the Domain

● Currently there is no license added at all

Add Users or connect LDAP

Build Dependencies

Create iOS Distribution Certificate

Upload iOS Provisioning Profile (wildcard or app-specific)


Upload Android Certificate

Upload Windows Phone Certificate

Connect Mac Build Node

Note: As long as the configuration is not yet finished, a message box with a **setup your site** link is displayed at the top of every page. You can return to the Configuration Assistant at any time during the configuration process by clicking this link. This message will no longer be shown when all app store clients have been built.

To use the Configuration Assistant

1. Do one of the following:
 - Click the **setup your site** link to access the Configuration Assistant directly.
 - Or proceed as follows:
 - i. Click  and then **Domains**.
 - ii. On the **All Domains** page, click the entry for the domain.
 - iii. On the **Domain Details** page, click **Configuration Assistant**.
2. Click the link that is shown in a configuration step (proceed from top to bottom) and specify all required information on the resulting page. This is explained in the following topics of this chapter.

Note: The following topics explain how to invoke a configuration step when not using the Configuration Assistant.


Adding the Mobile Administrator License File

You must provide a valid license file for Mobile Administrator. This is an XML file which is provided by Software AG. The expiration date and the number of named users supported by Mobile Administrator depends on the license file you use. You need a separate license file for each domain.

A license is either valid for an unlimited number of users or it has a user limit. The user limit applies to the number of named users who have logged in or used the Mobile Administrator instance in the last three months. As soon as the user limit is reached, users that have never logged in or have logged in more than three months ago will no longer be able to log in. Users who have logged in in the last three months will still be able to use Mobile Administrator, even if the user limit has been reached.

Users with the site-level permission **Manage Site** can always log in, regardless of the licensed number of users.

To add the license file

1. Click  and then **Domains**.
2. On the **All Domains** page, click the entry for the default domain.
3. On the **Domain Details** page, click **Edit Domain**.
4. Click **Browse** and upload the license file that you have received.
5. Scroll to the bottom of the **Domain Details** page and click **Update Site**.


The **Domain Details** page should now display information such as the following:

VALID (200 NAMED USERS)

Specifying the Domain Details

When you edit the details of the default domain (this is the same page on which you add the license file), you can specify information such as the company name, the administrator's email address and a logo.

To specify the domain details

1. Click  and then **Domains**.
2. On the **All Domains** page, click the entry for the default domain.
3. On the **Domain Details** page, click **Edit Domain**.
4. For now, specify only the following information:

- a. Company name
- b. Domain name
- c. Admin email
- d. Logo
- e. Certificate authority (CA) information

See ["Editing the Domain" on page 133](#) for detailed information on the above options. Information on other options that you can specify on this page is provided later in this chapter.

5. Click **Update Site**.



Adding Users

You can define users to Mobile Administrator by adding local users and/or by connecting to an LDAP server. In most cases, the users will be authenticated against an LDAP server.

Adding Local Users

When you add local users, you define the user names and passwords that are to be used to log in to Mobile Administrator. If required, you can also grant site-level permissions to these users.

To add local users

1. Click  and then **Users**.
2. On the **All Users** page, click .
3. On the resulting page, specify all required information for the user. See ["Adding a Local User" on page 142](#) for more detailed information.

Important: The **Active** check box is selected by default. Do not disable it. Otherwise the user will not be able to log in.

4. Click **Create User**.
5. Repeat the above steps for each local user that you want to add.

Connecting to an LDAP Server


You define LDAP users by connecting to an existing LDAP server. After you have created the connection to the LDAP server, the users can log in to Mobile Administrator with the user name and password credentials stored for them in the LDAP system.

When an LDAP user logs in to Mobile Administrator for the first time, all LDAP groups in which the user is defined as a member are automatically added to Mobile Administrator. These group memberships are automatically updated each time the user logs in to Mobile Administrator.

After a user has logged in to Mobile Administrator for the first time, an entry for this user is shown on the **All Users** page. If required, you can then grant site-level permissions to that user.

You cannot modify an LDAP user name or password with Mobile Administrator. This can only be changed through the LDAP directory.


To connect to an LDAP server

1. Click  and then **Domains**.
2. On the **All Domains** page, click the entry for the domain.
3. On the **Domain Details** page, click **Edit Domain**.
4. On the resulting page, scroll down to the heading **LDAP Configuration** and specify all required information. See "[Allowing Access for Users from an LDAP Directory](#)" on [page 135](#) for more detailed information.
5. Click **Update Site**.

Granting Site-Level Permissions to a User

For a local user, you can grant the site-level permissions directly when adding the user. For a user from an LDAP system, you can only grant them after the user has logged in to Mobile Administrator for the first time.

To grant site-level permissions to a user

1. Click  and then **Users**.
2. On the **All Users** page, click the entry for the user.
3. On the resulting page, click **Edit User**.
4. Scroll down to the heading **Permissions** and select the check boxes for the permissions that you want to grant to the user.
5. Click **Update User**.

Adding Code Signing Certificates for iOS

To prepare Mobile Administrator to build mobile applications for iOS, you must configure the build environment with the necessary code signing certificates and profiles. To obtain them, you have to enroll in the iOS Developer Program at <https://developer.apple.com/programs/ios/>.

You have to upload the following to Mobile Administrator:

- an iOS distribution certificate, and
- a provisioning profile that matches an iOS developer certificate.



Generating and Uploading an iOS Distribution Certificate

The following steps are required to obtain and upload an iOS distribution certificate:

1. Download a certificate signing request from Mobile Administrator.
2. Go to the iOS Provisioning Portal and request an iOS distribution certificate using the certificate signing request.
3. Download the generated iOS distribution certificate.
4. Upload the downloaded iOS distribution certificate to Mobile Administrator.

With Mobile Administrator, you can trigger these steps from a single page as described below.

To generate and upload an iOS distribution certificate

1. Click  and then **Developer Certificates**.
2. On the **All Certificates** page, click  and then **New iOS Distribution Certificate**.
3. Click **Certificate Signing Request** to download the certificate signing request.
4. Click the link for the iOS Provisioning Portal, sign in with your Apple ID, generate an iOS distribution certificate using your certificate signing request, and then download the generated iOS distribution certificate.
5. Click **Browse** and select the iOS distribution certificate that you have downloaded.
6. Click **Upload Certificate**.

Uploading an iOS Provisioning Profile

The following steps are required to obtain and upload an provisioning profile:

1. Go to the iOS Provisioning Portal and request an iOS provisioning profile.
2. Download the generated iOS provisioning profile.
3. Upload the downloaded iOS provisioning profile to Mobile Administrator as described below.

If Mobile Administrator cannot find a matching iOS developer certificate, the upload of the provisioning profile will fail.

To upload an iOS developer provisioning profile

1. Click  and then **Provisioning Profiles**.

2. On the **All iOS Provisioning Profiles** page, click **+**.
3. Click **Browse** and select the mobile provisioning profile.
4. Click **Upload**.

Adding Code Signing Certificates for Android

To prepare Mobile Administrator to build mobile applications for Android, you must configure the build environment with the necessary certificates.

After the installation of Mobile Administrator, a certificate with the name "Default Android Distribution Certificate" is automatically available. You can optionally upload a different code signing certificate (developer certificate) for Android.

Uploading a Developer Certificate for Android

See <http://developer.android.com/tools/publishing/app-signing.html> for information on how to generate an Android developer certificate.

To upload an Android developer certificate

1. Click **⚙** and then **Developer Certificates**.
2. On the **All Certificates** page, click **+**.
3. Click **Browse** and select the developer certificate (.p12 file only).
4. Enter the PKCS12 password.
5. Select **Android** as the platform.
6. Click **Upload**.

Adding Code Signing Certificates for Windows Phone

To prepare Mobile Administrator to build mobile applications for Windows Phone, you must configure the build environment with the necessary tokens and certificates. You have to upload the following:


- a Windows Phone 8 application enrollment token, and
- a code signing certificate (developer certificate) for Windows Phone.

Uploading the Windows Phone 8 Application Enrollment Token

When you register for the Windows Phone Dev Center, you receive a Windows Phone 8 application enrollment token file. You use this file to configure Windows Phone 8 devices for the installation of enterprise applications.

The token that you upload needs to be installed on every Windows Phone 8 device prior to the installation of any apps, signed with your Windows Phone certificate. On a Windows Phone device, you can locate the download link for the token when visiting the mobile logon page.



To upload a Windows Phone 8 application enrollment token

1. Click  and then **Domains**.
2. On the **All Domains** page, click the entry for the domain.
3. On the **Domain Details** page, click **Edit Domain**.
4. Locate the **Windows Phone 8 application enrollment token** option, click **Browse** and select the AETX file.
5. Go to the bottom of the page and click **Update Site**.

Uploading a Developer Certificate for Windows Phone

See <http://msdn.microsoft.com/en-us/library/windows/apps/jj206943%28v=vs.105%29.aspx> for information on how to acquire a certificate. You must upload a file in the P12 format which contains a certificate and a private key. Both must match.

To upload a Windows Phone developer certificate

1. Click  and then **Developer Certificates**.
2. On the **All Certificates** page, click .
3. Click **Browse** and select the developer certificate (.p12 file only).
4. Enter the PKCS12 password.
5. Select **Windows Phone** as the platform.
6. Click **Upload**.



Adding Code Signing Certificates for Windows 8/RT

To prepare Mobile Administrator to build mobile applications for Windows 8/RT, you must configure the build environment with the necessary certificates. You have to upload a code signing certificate (developer certificate) for Windows 8/RT.

Uploading a Developer Certificate for Windows 8/RT

See <http://msdn.microsoft.com/en-us/library/vstudio/hh691189%28v=vs.110%29.aspx> for information on how to acquire a certificate. You must upload a file in the P12 format which contains a certificate and a private key. Both must match.

To upload a Windows 8/RT developer certificate

1. Click  and then **Developer Certificates**.
2. On the **All Certificates** page, click .
3. Click **Browse** and select the developer certificate (.p12 file only).
4. Enter the PKCS12 password.
5. Select **Windows 8/RT** as the platform.
6. Click **Upload**.

Connecting Build Nodes


With Mobile Administrator, builds run in the cloud without developers having to run build environments for all platforms on their developer machines. You can connect one or more remote build nodes. A Mac OS X build node supports building apps for iOS and Android. A Windows 8 build node supports building apps for Windows Phone and Windows RT.

Note: Make sure that Mobile Designer and any required SDKs have already been installed on the machine that you want to use as the build node.

Connecting a Build Node for iOS and Android

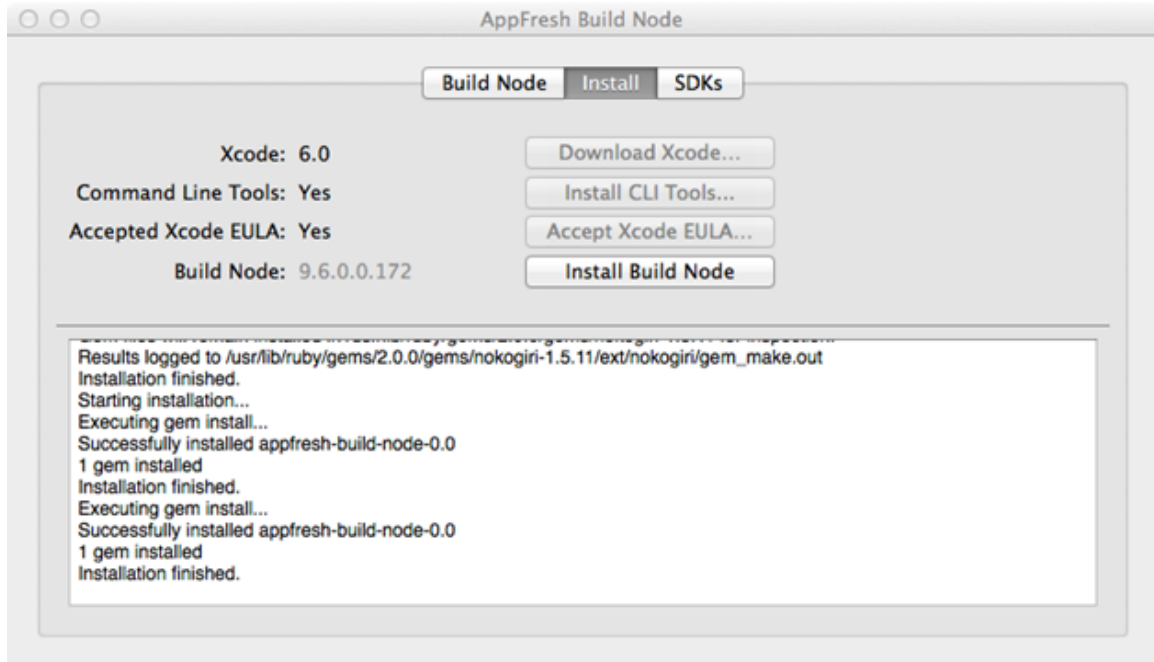
Apps for iOS and Android are built on Mac OS X build nodes. To connect such a build node, you first have to download a zip file from Mobile Administrator as described below. When you extract the downloaded file, you can launch the AppFresh Build Node wizard in which you can then specify all required information for installing the build node and connecting it to a Mobile Administrator instance.

To connect a build node for iOS and Android on Mac OS X

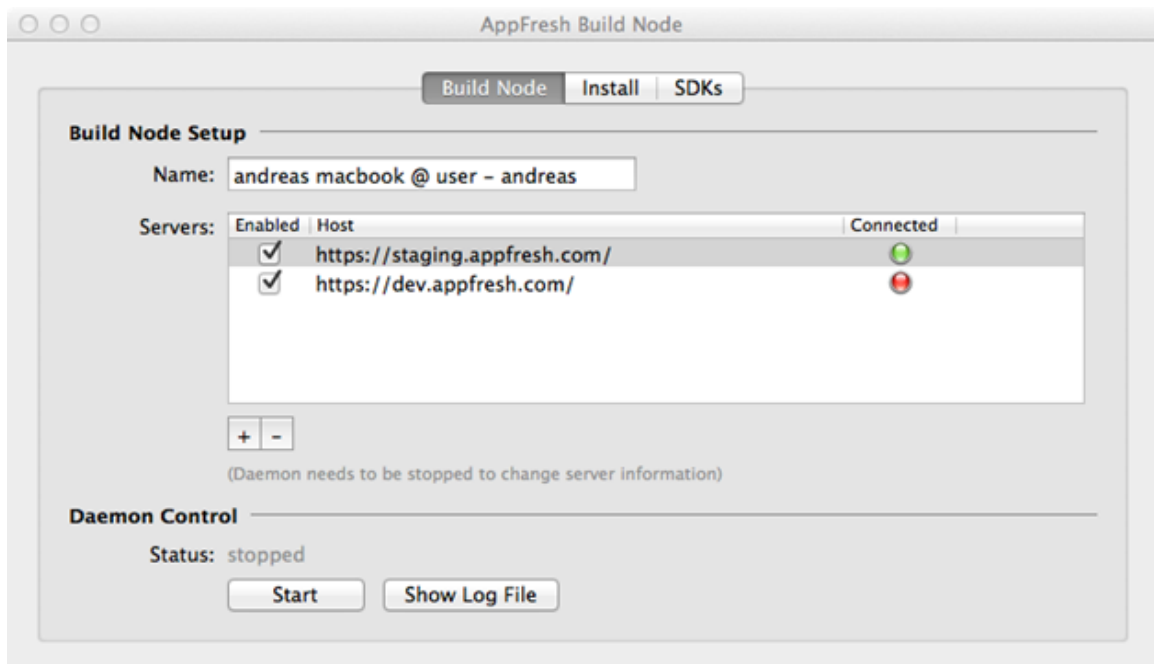
1. Click  and then **Build Nodes**.
2. Scroll down to the bottom of the **All Build Nodes** page.
3. Click the link for the zip file and download this file.

Normally, you download this file directly to the machine on which you want to set up the build node. Otherwise, you have to copy it to that machine.

4. Extract the downloaded file.
5. Launch the extracted application to invoke the AppFresh Build Node wizard.
6. Go to the **Install** tab of the wizard and click the available buttons to perform the corresponding steps (download Xcode, install command line tools, accept Xcode EULA, and install build node).



7. Go to the **Build Node** tab of the wizard.



8. To connect the newly installed build node with your Mobile Administrator instance, click **+**.

The following is shown:

9. Specify the Mobile Administrator host name (without https://), your user name and password, and then click **Add Host**.
10. Make sure the newly added host name shows up in the **Servers** list of the **Build Node** tab.
11. Specify a recognizable identifier for the build node in the **Name** field. This name will be shown in Mobile Administrator as the build node name.
12. Click **Start**.

A green icon in the **Connected** column will indicate that the build node has been connected successfully.

Note: If you want to obtain debug information about the build node, click **Show Log File** and check the log.

13. Optional. Go to the **SDK** tab of the wizard to view the installed SDKs that have been detected on the build node.
14. Go back to Mobile Administrator. The **All Build Nodes** page will now show an entry for the new build node.

Connecting a Build Node for Windows Phone and RT

Apps for Windows Phone and RT are built on Windows 8 Pro build nodes. To connect such a build node, you first have to download an exe file from Mobile Administrator as described below. When you extract the downloaded file, you can launch the AppFresh Windows wizard in which you can then specify all required information for installing the build node and connecting it to a Mobile Administrator instance.

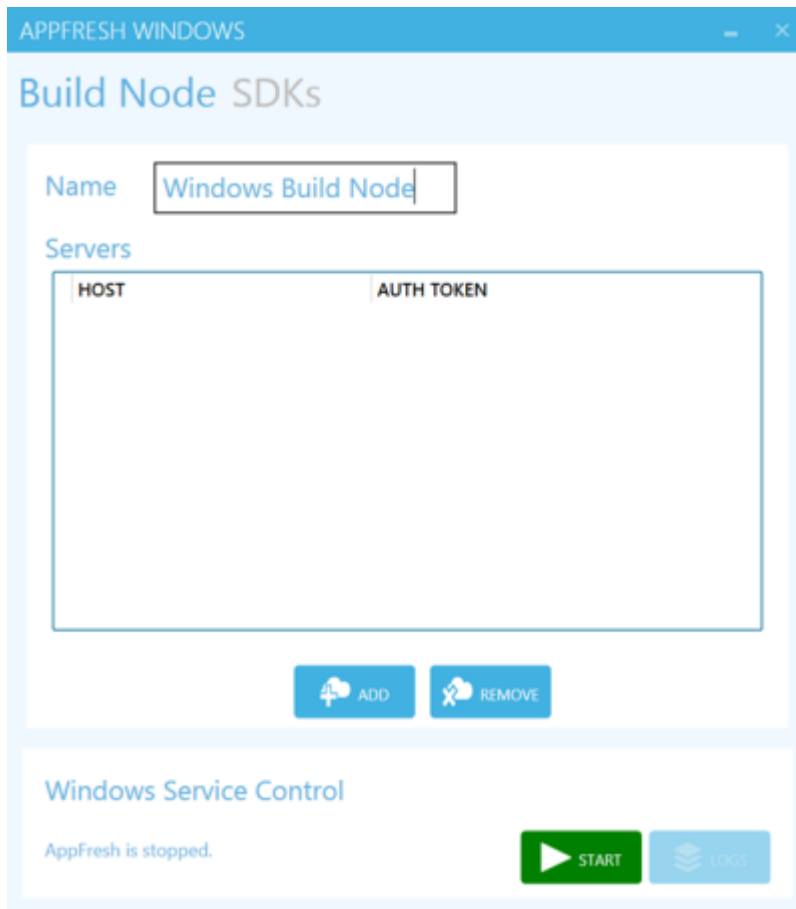
To connect a build node for Windows Phone and RT on Windows 8 Pro

1. Click and then **Build Nodes**.
2. Scroll down to the bottom of the **All Build Nodes** page.
3. Click the link for the exe file and download this file.

Normally, you download this file directly to the machine on which you want to set up the build node. Otherwise, you have to copy it to that machine.

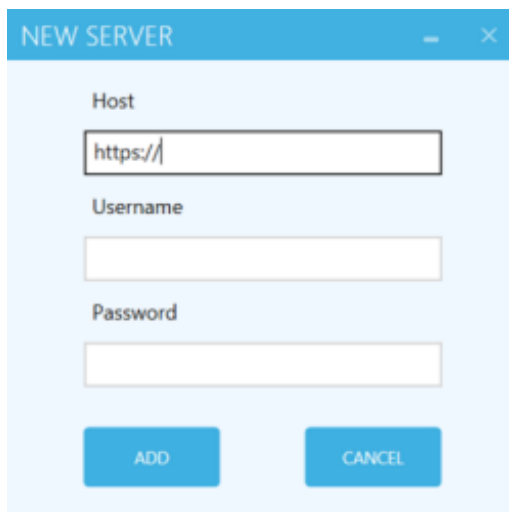
4. Run the downloaded installer file and follow the instructions for installing the build node.

5. Launch the build node application to invoke the AppFresh Windows wizard.

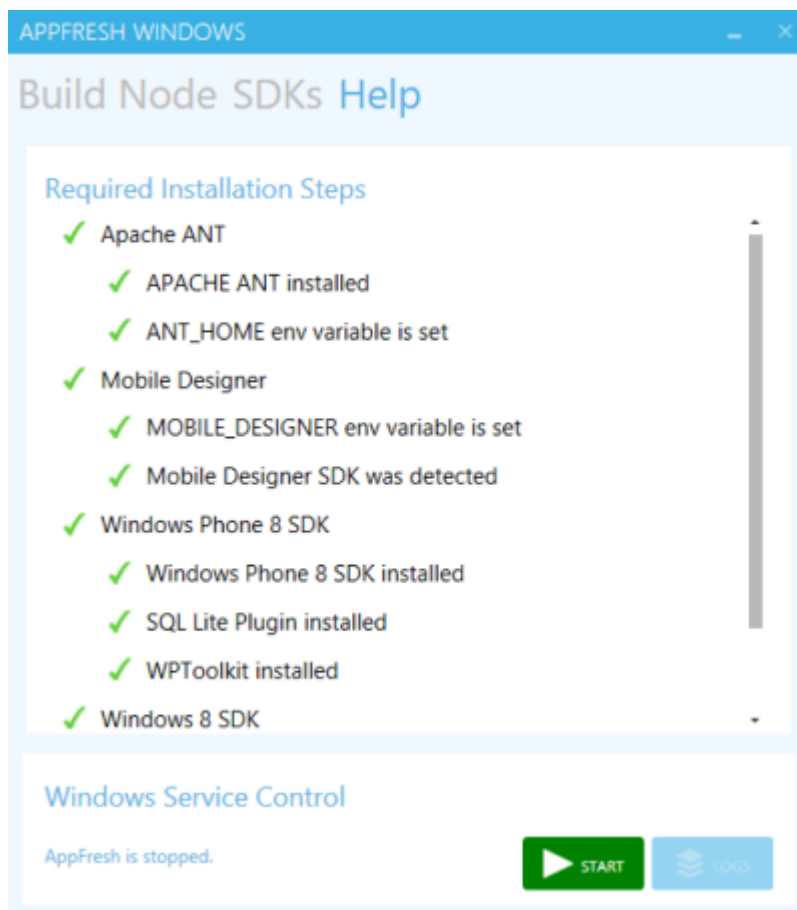


6. To connect the build node to your Mobile Administrator instance, click **Add** on the **Build Node** tab.

The following is shown:



7. Specify the Mobile Administrator host name (without https://), your user name and password, and then click **Add**.
8. Make sure the newly added host name and authentication token show up in the **Servers** list.
9. Specify a recognizable identifier for the build node in the **Name** field. This name will be shown in Mobile Administrator as the build node name.
10. Optional. Go to the **SDKs** tab of the wizard to view the installed SDKs that have been detected on the build node.
11. Optional. Go to the **Help** tab of the wizard to make sure that all required software has been installed on the build node.



12. Click **Start**.
13. Go back to Mobile Administrator. The **All Build Nodes** page will now show an entry for the new build node.

Creating and Launching Build Configurations for the App Store Client

After you have uploaded the required certificates and profiles for your platforms and after you have connected the build nodes, you can build mobile applications with Mobile Administrator. One of the first apps that you want to build is the app store client for each mobile platform on which you want to offer your apps for download. Building the app store client is optional, however, it is very convenient for your users to browse and download your apps. As an alternative, your users can also access the app store website via the browser on their mobile devices.

Important: The app store client is required if you want to use mobile device management (MDM) on iOS or Android. In this case, the users have to install the app store client on their mobile devices, and they have to allow the mobile device management in the settings of the app store client. See also ["Allowing the Mobile Device Management" on page 197](#).

Note: Mobile device management is not yet supported on Windows Phone platforms.

You have to create a build configuration for each platform on which you want to make the app store client available.


Creating the Build Configuration for the iOS Platform

When you create a build configuration for iOS, you have to specify a provisioning profile that you have already uploaded. The bundle ID associated with the uploaded provisioning profile must match the iOS bundle ID configured for the app store client.

Verifying the Bundle ID for the App Store Client

It is recommended that you verify the bundle ID of the app store client before creating the build configuration.



To verify the bundle ID for the app store client

1. Click  and then **App Store Client**.
2. Click **Edit**.
3. On the resulting page, scroll down to the heading **iOS**. Check the bundle ID that is shown there. If necessary, update the bundle ID to a value that matches your provisioning profile and click **Update App**.

Creating the iOS Build Configuration for the App Store Client

The procedure below just mentions the minimum options that are required to create the build configuration. For detailed information on all options that can be set, see ["Adding a Build Configuration" on page 91](#).

To create the iOS build configuration for the app store client

1. Click  and then **App Store Client**.
2. Click **Build** on the left side.
3. On the **Build Configurations** tab, click .
4. From the **Platform** drop-down list box, select **iOS**.
5. Scroll down to the heading **iOS** and make sure that the iOS provisioning profile that you have uploaded is selected in the corresponding drop-down list box.

Note: If the drop-down list box does not contain any of your iOS provisioning profiles, none of them matches the iOS bundle ID of the app store client.



6. Click **Create Build Configuration**.

Creating the Build Configuration for the Android Platform

When you create a build configuration for Android, you have to specify a developer certificate that you have already uploaded.

The procedure below just mentions the minimum options that are required to create the build configuration. For detailed information on all options that can be set, see ["Adding a Build Configuration" on page 91](#).

To create the Android build configuration for the app store client



1. Click  and then **App Store Client**.
2. Click **Build** on the left side.
3. On the **Build Configurations** tab, click .
4. From the **Platform** drop-down list box, select **Android**.
5. Scroll down to the heading **Android** and make sure that the developer certificate that you have uploaded is selected in the corresponding drop-down list box.
6. Click **Create Build Configuration**.

Creating the Build Configuration for the Windows Phone Platform

When you create a build configuration for Windows Phone, you have to specify a code signing certificate that you have already uploaded.

The procedure below just mentions the minimum options that are required to create the build configuration. For detailed information on all options that can be set, see ["Adding a Build Configuration" on page 91](#).

To create the Windows Phone build configuration for the app store client



1. Click  and then **App Store Client**.
2. Click **Build** on the left side.
3. On the **Build Configurations** tab, click  .
4. From the **Platform** drop-down list box, select **Windows Phone**.
5. Scroll down to the heading **Windows Phone** and make sure that the code signing certificate that you have uploaded is selected in the corresponding drop-down list box.
6. Click **Create Build Configuration**.

Creating the Build Configuration for the Windows 8/RT Platform

When you create a build configuration for Windows 8/RT, you have to specify a code signing certificate that you have already uploaded.

The procedure below just mentions the minimum options that are required to create the build configuration. For detailed information on all options that can be set, see ["Adding a Build Configuration" on page 91](#).

To create the Windows 8/RT build configuration for the app store client


1. Click  and then **App Store Client**.
2. Click **Build** on the left side.
3. On the **Build Configurations** tab, click  .
4. From the **Platform** drop-down list box, select **Windows 8/RT**.
5. Scroll down to the heading **Windows 8/RT** and make sure that the code signing certificate that you have uploaded is selected in the corresponding drop-down list box.
6. Click **Create Build Configuration**.

Launching the Build Configurations for the App Store Client

Afer you have created the build configurations for the app store client, you have to launch them for all platforms.

Other than for normal apps, you need not specify a source file for the app store client when launching the build configurations. The app store client will be built using the sources that are shipped with Mobile Administrator.

To launch the build configurations for all platforms

1. Click  and then **App Store Client**.
2. Click **Build** on the left side.
3. On the **Build Configurations** tab, select the check boxes for all build configurations that you have created.
4. Click **Launch Selected Build Configurations**.



Mobile Administrator generates a build job for each selected build configuration (and thus for the platforms on which you want to make available the app store client).

The status of each build job is shown on the **Build Jobs** tab. The build jobs remain in **Initializing** status for a while as Mobile Administrator creates the source code for the app store client. When in **Pending** status, the build jobs are ready to be processed by any online build nodes. When in **Running** status, the build job is processed. When a build job has successfully finished, its status is **Success**.

Note: If something went wrong, the status is **Error**. If you want to get detailed information on the error, click the entry for the build job and then click **Show Errors** which is shown at the bottom of the resulting page.

When the build jobs have finished successfully, you can go to the **Versions** page of the app store client to view build configuration information, such as platform, version, and date.

You can now install the app store on a mobile device. For more information, see ["Using the App Store on a Mobile Device" on page 193](#).

Note: You can specify a different name or icon for the app store client, or you can enter your individual description and contact information as for any other app. See also ["Editing an App" on page 65](#). However, keep in mind that you have to display the app details via the **App Store Client** command in the  menu. It is not possible to change the app store client via  **Manage Apps**.

Configuring the Mobile Device Management


Before you can use the mobile device management (MDM), you have to provide the required information in Mobile Administrator. For iOS, you have to upload an MDM certificate. For Android, you have to specify a Google Cloud Messaging (GCM) API key.

Note: The mobile device management is not supported on Windows Phone platforms.

Uploading an MDM Certificate for iOS

To support mobile device management (MDM) on iOS devices, you have to upload an MDM certificate signed by Apple.


To upload an MDM certificate for iOS

1. Click  and then **Domains**.
2. On the **All Domains** page, click the entry for the default domain.
3. On the **Domain Details** page, scroll down to the heading **MDM Certificates**.
4. Click **New Certificate**.
5. Click **Certificate Signing Request** to download the certificate signing request.
6. Click the link for the Apple Push Certificates Portal, sign in with your Apple ID, create a new push certificate using your certificate signing request, and then download the push certificate.
7. Click **Browse** and select the push certificate that you have downloaded.
8. Click **Upload Certificate**.

Specifying a GCM API Key for Android

A Google Cloud Messaging (GCM) API key is required if you want to support mobile device management (MDM) and push notifications on Android devices. For more information on how to obtain such a key, see <http://developer.android.com/google/gcm/gs.html>.

To specify the GCM API key for Android

1. Click  and then **Domains**.
2. On the **All Domains** page, click the entry for the default domain.
3. On the **Domain Details** page, click **Edit Domain**.
4. In the **GCM API Key** field, specify the API key.
5. Click **Update Site**.

3 Managing Apps

■ Overview	48
■ The All Applications Page	49
■ Organizing Apps in Categories	50
■ Adding an App	53
■ Displaying an App	61
■ Managing the App Details	63
■ Managing the Versions of an App	68
■ Managing the Resources of an App	76
■ Managing the Permissions of an App	83
■ Managing the Builds of an App	86
■ Managing the Devices on Which the App Can be Installed	100
■ Managing the Push Notifications for an App	102
■ Using the Apple App Store Volume Purchase Program (VPP)	104
■ Viewing the App Analytics	107

Overview

This chapter explains how to add apps to your app store and how to sort them into categories.

To add new apps (including all app-specific rights for the newly created app) and to manage apps (including all permissions for the app), you need the site-level permissions **Add Apps** and **Manage Apps**. See also "[Overview of Site-Level Permissions](#)" on page 141.

It is also possible to grant permissions for single apps to certain users. These are the so-called application-level permissions. When a user has been granted one or more of these permissions, the user will also be able to manage certain aspects of the app, for example, edit the metadata of the app or build a new app version. See also "[Overview of Application-Level Permissions](#)" on page 84.

You can add apps with ready-to-run app versions to Mobile Administrator and you can also add apps for which the app versions are still to be built. In the latter case, you have to set up build nodes and create build configurations for all platforms on which the app is to be made available. The app version for a platform will be built when you launch the corresponding build configuration.

When you build app versions with Mobile Administrator, you can make available the source code in two different ways:

- You can upload the source code as a zip file (for example, when you do not use a repository and all of your files are stored locally). The uploaded zip file will then be used when a new build is launched.
- You can instruct Mobile Administrator to fetch the source code automatically from a repository each time a new build is launched. In this case, you have to specify all required information such as the URL to the repository and your credentials.

In addition to the apps that you have developed yourself, you can also mirror apps that have been published in a vendor store such as the Apple App Store or Google Play. In the case of Apple, you can also purchase apps in volume so that your users do not have to pay for them.

You can remotely install and update apps over the air on the devices on which the mobile device management has been allowed, and you can send push notifications to registered devices.

Usage information on an app also provided. This is helpful if you want to optimize an app.



The All Applications Page

When you click  **Manage Apps**, the **All Applications** page is shown which lists all currently defined apps. You can then:

- Add new apps that are to be published into your app store. See ["Adding an App" on page 53](#).
- Click an existing app to view it. You can then change different aspects of the app. For example, you can build new versions of the app or define the users who are allowed to use the app. See ["Displaying an App" on page 61](#).
- Define new categories into which the apps are to be sorted in your app store. See ["Adding a Category" on page 50](#).

Note: The category in which an app appears is defined in the app details. If you want to change the category, you have to edit the app. See ["Editing an App" on page 65](#).


The **All Applications** page provides two different views. You can switch between these views by clicking the corresponding icon at the top of the page:

Icon	View Name	Description
	List view	<p>In this view, the apps are listed one below another and a check box is provided for each app. This allows you to delete or batch-edit selected apps.</p> <p>You can sort the apps by clicking on a header (for example, you can sort them by platform).</p> <p>At the bottom of the page, you can define the number of entries to be shown on the page, and you can click a page number to go to that page.</p> <p>If you want to limit the number of apps that are shown, you can enter a character or a string of characters in the Filter box that is shown at the top of the page. For example, if you enter <code>j</code>, all apps are shown which have this letter at any position in the app name. Or if you enter <code>first</code>, all apps are shown which have this string within the app name. See also "Filtering Lists" on page 22.</p>
	Grid view	<p>In this view, icons are shown for the apps (as in the app store) and the apps are sorted into categories. If you want to edit, for example, the name or description of an existing category, you have to go to this view.</p>

Icon	View Name	Description
		As in the app store, a search box is provided. Other than with the above-mentioned Filter box, the search function looks for the provided string in the name, description and short description of the apps. This also includes information such as the copyright or the supported platforms. To start the search, you have to press ENTER.

Organizing Apps in Categories

In the app store, the apps are normally sorted into categories. If you want to assign a new or existing app to a category, this category has to be created first.

If you want to find out which apps have not yet been assigned to a category, click  **Manage Apps**. In the grid view, the apps that have not yet been assigned to a category are shown under the heading **Uncategorized Apps** (near the bottom of the page). In the list view, the corresponding entry in the **Category** column is empty when an app has not yet been assigned to a category.






Adding a Category

You can create the following types of categories:

- Normal categories into which the apps are assigned manually.
- Smart categories into which the apps are sorted automatically according to specific filter criteria. This requires that the option **Smart Filter** has been defined in the category details.

Each newly added category is immediately shown in the grid view of the **All Applications** page. On the **App Store** page, however, a new category is only shown after an app has been assigned to the category. Keep in mind that on the mobile device, a category shows only the app versions which have been built for the platform on which your device is running.

To add a category

1. Click  **Manage Apps**.
2. Do one of the following:
 - In the list view () , click  and then **Add Category**.
 - Or in the grid view () , click  **Category**.
3. On the resulting page, specify the following information:

Option	Description
Name	Type a name for the new category.
Custom order	<p>Select a number from 0 through 99 to define the sequence in which you want to present your categories. For example, you have 3 categories. The category with the number 0 is shown as the very first category. The category with the number 20 is shown as the second category. And the category with the number 60 is shown as the last category. When you now add a new category that you want to show directly after the first category in the list, you can define any number from 1 through 19 for that category.</p> <p>If you want to arrange your categories alphabetically, just use the same number (for example, 50) for all of them.</p>
Icon	Click Browse to select an icon that is to be shown in front of the category name. This should be a PNG file with a size of 96 x 96 pixels. On a mobile device, the icon will be shown on the start page.
Description	Optional. Type a description of the category. On a mobile device, this description will be shown on the start page of the app store client, below the category name.
Background color	<p>By default, the background color for a category is white (#FFFFFF). The background color is only shown in the app store client on a mobile device, on the start page which lists the available categories.</p> <p>Click this text box if you want to select a background color from a drop-down menu or type the HTML code for the color (for example, #FFFF00 for yellow). The currently defined color is always shown to the right of the text box.</p>
Overlay image	Optional. Click Browse to define an image that is to be used as a teaser. This should be a PNG file with the appropriate size for the native devices (for example, a width of 1080 pixels for iPhone 6). This image is only shown on the mobile device, on the start page. If defined, the overlay image is shown instead of the category name, description and background color.

Option	Description
Smart Filter	<p>Optional. Use this option to define a smart category into which the apps are sorted automatically according to the filter criteria that you define here.</p> <p>If you need help, click the ? button which is shown to the right of the text box. For more details, see the query language reference at https://github.com/wvanbergen/scoped_search/wiki/query-language.</p> <p>The smart categories are only shown in the grid view of the All Applications page.</p>

If you notice that you have selected a wrong icon or overlay image, just click **Browse** and select a different file.

4. Click **Create App Category**.



The resulting page informs you that the new category does not yet contain any apps. A link is provided for adding one. See also "[Adding an App](#)" on page 53.

If you want to add already existing apps to the new category, you have to edit the app and define the category. See "[Editing an App](#)" on page 65.

Editing a Category


You can edit all categories. For example, you can change the category name, description or icon.

To edit a category

1. Click  **Manage Apps**.
2. Go to the grid view (.
3. Click the name of the category that you want to edit.
4. Click **Edit Category**.
5. On the resulting page, specify or change all required information. For detailed information on the available options, see "[Adding a Category](#)" on page 50.
6. Click **Update App Category**.

Deleting a Category

If a category is no longer required, you can delete it.

Deleting a category does not delete the apps that are contained in the category. In the grid view () , the apps will then be listed under "Uncategorized Apps".

To delete a category

1. Click **Manage Apps**.
2. Go to the grid view (☐☐).
3. Click the name of the category that you want to delete.
4. On the resulting page, click **Delete Category**.
A dialog box appears, asking whether you are sure.
5. Click **OK** to confirm the deletion.

Adding an App

An app can be published into the enterprise app store via a variety of means. For example, you can use Mobile Administrator to upload it directly from a binary, or you can have it uploaded automatically from webMethods Mobile Designer. Mobile Designer can control build nodes in order to manage the building of projects directly.

When you add an app with Mobile Administrator, you first have to decide how you would like to create the new app. You can add application binaries that have been developed, for example, with Mobile Designer. Or you can add apps from an existing app store. You can also just create a shell for an app that is yet to be developed.

All Applications --> New Application

New Application

Choose how you would like to create a new application:

- I have an application binary
- I have an exported application and want to import it
- I want to add an app from the Apple App Store
- I want to add an app from the Google Play Store
- I want to add an app from the Windows Phone Store
- I want to add an app from another webMethods Mobile Administrator Instance
- I will enter the application details manually

Depending on your selection, different options are shown that you have to specify. For detailed information, see the appropriate section later in this documentation.

Each app that you add will immediately be visible in Mobile Administrator. In the app store client, however, an app will only be visible if there is a stable version for this app.

The sections below describe typical scenarios for adding an app to your app store.

Scenario 1: You already have an application binary

You have developed your app (for example, with Mobile Designer) and you have the ready-to-upload binaries for all platforms on which the app can be used (for example, an iOS .ipa file and an Android .apk file). A build configuration is not required in this case.

Proceed as follows:

1. Add an app with the option **I have an application binary** and then upload a binary. See ["Adding an Application Binary" on page 56](#).

Using this option, you can only upload a single binary (for example, the above-mentioned .ipa file). Additional binaries can be uploaded from the **Versions** page of the app as described below.

2. Edit the app details. For example, specify the final app name, provide a description, an icon, screenshots, and assign the app to an existing category. See ["Editing an App" on page 65](#).

3. Go to the **Versions** page of the app and do the following:

- a. Upload the binaries for all other platforms (for example, the above-mentioned .apk file).
- b. Make sure that the product stage is stable.

See ["Managing the Versions of an App" on page 68](#).

Depending on the platform, some policies are already predefined. For example, for Android it is predefined that the app usage is to be logged and that app crashes are to be reported.

4. Go to the **Permissions** page of the app. Make sure that your users will be able to download your app. In most cases, you will allow them to view and download stable versions. See ["Managing the Permissions of an App" on page 83](#).
5. If you have selected a stable product stage, the new app is now visible in your app store and can be installed on the mobile devices of your users. See ["Using the App Store on a Mobile Device" on page 193](#).

Scenario 2: You do not yet have ready-to-upload binaries

You want to upload a Mobile Designer project and let Mobile Administrator build the binaries for you (for example, for Android and iOS). In this case, a build configuration is required. This scenario assumes that your source code is not stored in a source code repository. It assumes instead that all required source code files are stored locally on your machine.

Proceed as follows:

1. Add an app with the option **I will enter the application details manually**. Specify all required options such as the app name, description, category and icon. Specify the

bundle ID for each platform on which you want to make the app available. This must be the same bundle ID as defined in the source. Otherwise, the build will fail. See ["Specifying the Details for the New App Manually" on page 58](#).

2. If you want to add screenshots, edit the app after it has been created. See ["Editing an App" on page 65](#).
3. Go to the **Permissions** page of the app. Make sure that your users will be able to download your app. In most cases, you will allow them to view and download stable versions. See ["Managing the Permissions of an App" on page 83](#).
4. As no binaries have been uploaded yet, the app is not yet installable. Therefore, go to the **Build** page of the app. On the **Build Configurations** tab, add a new build configuration for each platform (for example, one for iOS and another for Android). See ["Adding a Build Configuration" on page 91](#). Make sure to specify the following in each build configuration:
 - a. Select the platform for which you want to create the build configuration.
 - b. Select a build node.
 - c. Select the product stage (stable or unstable).
 - d. Specify platform-specific information such as the iOS provisioning profile or Android developer certificate.
 - e. Select **Build using webMethods Mobile Designer** and enter a target name, that is, the "target device" as defined in Mobile Designer.
 - f. Define the app policies. For example, you can define that the app usage is to be logged and that app crashes are to be reported.
5. Check the **Build Configurations** tab. An entry should now be shown for each platform for which you have created a build configuration. See ["Managing the Build Configurations of an App" on page 87](#).
6. Do the following on the **Build Configurations** tab:
 - a. Specify a version number.
 - b. If you want, you can also specify a build number. If you do not specify a build number, is automatically increased when you launch the build configuration.
 - c. Click **Browse** and upload the zip file containing the source code.
 - d. Click **Launch Selected Build Configurations**.
7. Go to the **Build Jobs** tab and view the job output. Make sure that the build jobs for the different platforms have been run successfully. See ["Managing the Build Jobs of an App" on page 97](#).
8. Go to the **Versions** page of the app. The result of each build job is a new app version on this page. See ["Managing the Versions of an App" on page 68](#).
9. If you have selected a stable product stage, the new app is now visible in your app store and can be installed on the mobile devices of your users. See ["Using the App Store on a Mobile Device" on page 193](#).






Adding an Application Binary

You can upload packaged mobile applications in the file formats listed in the section ["Installation and Prerequisites" on page 14](#).

The uploaded app has the same name as defined in the binary.

Note: Using this option, you can only upload a single binary. If you want to add the binaries for other platforms to your app, go to the **Versions** page of the app and upload the binaries there. See ["Managing the Versions of an App" on page 68](#).






To add an application binary

1. Click  **Manage Apps**.
2. Do one of the following:
 - In the list view () , click .
 - Or in the grid view () , click .
3. On the resulting page, click **I have an application binary**.
4. Click **Browse**.
5. In the resulting dialog box, select the binary to be uploaded.
6. Click **Upload**.

Importing an App

You can import any app that has previously been exported with Mobile Administrator. The exported app is a zip file which contains all metadata of the app and all of its versions. See also ["Exporting an App" on page 66](#).

To import an app

1. Click  **Manage Apps**.
2. Do one of the following:
 - In the list view () , click .
 - Or in the grid view () , click .
3. On the resulting page, click **I have an exported application and want to import it**.
4. Click **Browse** and select the zip file to be imported.
5. From **Existing Items**, select one of the following:
 - **Merge**. Default. If there are conflicts with existing items, the items are merged.

- **Skip.** If there are conflicts with existing items, the conflicting items are skipped and processing continues with the next item.
6. Click **Import**.






Adding an App from a Vendor App Store

You can mirror apps that are published in the Apple App Store, Google Play, and Windows Phone Store. This is useful if you want to offer your employees or customers a selection of recommended or pre-approved apps. This is also useful if a volume purchase license from the Apple App Store has been obtained for a selection of apps; see also "[Using the Apple App Store Volume Purchase Program \(VPP\)](#)" on page 104. In this case, the employees can download the apps without having to pay anything.

When the user downloads an app from a vendor store, the download button indicates from where the app will be downloaded (for example, **Download via Google Play**).

After you have added an app from a vendor app store, you can edit it as any other app. For example, you can change its description, add contact information, assign it to a category, or delete screenshots.

To add an app from a vendor app store

1. Click  **Manage Apps**.
2. Do one of the following:
 - In the list view () , click .
 - Or in the grid view () , click  **App**.
3. On the resulting page, click one of the following:
 - I want to add an app from the Apple App Store**
 - I want to add an app from Google Play**
 - I want to add an app from the Windows Phone Store**
4. Type the ID of the app.






Tip: Invoke the app in the vendor app store and then copy its ID from the URL.

5. Click **Pull App**.

Adding an App from Another Mobile Administrator Instance

You can add an app that is currently available in another instance of Mobile Administrator. This is helpful, for example, if you have set up an app for testing purposes in a test environment and you now want to make the app available in your official app store so that it can be downloaded by your employees or customers.

To add an app from another Mobile Administrator instance

1. Click  **Manage Apps**.
2. Do one of the following:
 - In the list view () , click  .
 - Or in the grid view () , click  **App** .
3. On the resulting page, click **I want to add an application from another webMethods Mobile Administrator instance**.
4. Type the URL of the Mobile Administrator instance from which you want to add the app.
5. Copy the access token from the Mobile Administrator instance from which you want to add the app, and paste it in the corresponding text box. You can find the access token in the user profile.
6. Click **Show App List**.






The apps from the specified Mobile Administrator instance are now listed.
7. Select the check box for the app that you want to add.
8. Click **Pull from Remote Instance**.

Specifying the Details for the New App Manually

You can specify the details for a new apps manually, for example, if the app has not yet been developed and you want to create a shell that you can then call up with webMethods Mobile Designer for further processing, or if the app has already been developed and you have ready-to-build source code, but the app has not yet been built for a specific platform.

A new app is not yet installable if the required binary has not been defined. After you have created the new app, you have to define all required build configurations (see ["Adding a Build Configuration" on page 91](#)).

To specify the details for the new app manually

1. Click  **Manage Apps**.
2. Do one of the following:
 - In the list view () , click  .
 - Or in the grid view () , click  **App** .
3. On the resulting page, click **I will enter the application details manually**.
4. Specify the following information:

Option	Description
Name	Type a name for the new app. The name may contain letters, digits or underscore characters. This is the name under which the app is listed in the app store client.
Short description	Optional. Type a short description of the app. On the mobile device, this description will be shown in the list of apps in the app store client.
Description	Optional. Type a more detailed description of the app. On the mobile device, this description will be shown when the user displays the app in the app store client.
Identifier	Optional. The identifier that is to be shown in the URL is automatically created based on the app name that you enter. If you want, you can type a different identifier.
Contact name	Optional. The first and last name defined in your user profile is automatically provided as the contact information. If you want, you can define a different name. On the mobile device, this name will be shown when the user displays the app in the app store client.
Contact email	Optional. The email address defined in your user profile is automatically provided. The users of the app can send mail to that address. If you want, you can define a different email address. On the mobile device, this email address will be shown when the user displays the app in the app store client.
Copyright	Optional. Type your copyright information. On the mobile device, this information will be shown when the user displays the app in the app store client.
Product category	Select the category to which this app is to belong. All currently defined categories are provided for selection. On the mobile device, the category is shown on the start page of the app store client.
Tags	Enter any tags, separated by a comma. The tags are used to determine the "Related Apps" that are shown when the user displays an app in the app store. They are also considered when searching the app store or when filtering the apps.

Option	Description
Downloads are public	If not selected (default), the app can only be downloaded via the app store. If selected, the app can also be downloaded anonymously via the browser on the device.
Available on managed devices only	If not selected, the app can be installed by all users who can log in to your app store. If selected, the app can only be installed on devices on which the mobile device management has been allowed in the app store client.
Hidden from app store listing	If not selected, the app will be shown in your app store as soon as a version has been built. If selected, the app will not be shown in your app store. This is helpful, for example, if the app still needs to be developed and you want to make it visible at a later point in time.
Icon	Optional. Click Browse and upload the icon that is to be shown for this app. This should be a PNG file with a size of 96 x 96 pixels. If you do not upload an icon, a default icon will be used.

- For each platform on which you want to make the app available, specify the **Bundle ID** (this is the unique identifier for the binary). You have to specify the same bundle ID as defined in the source. Otherwise, the build will fail.
- Specify any additional options that may be necessary. The additional options are described in the following table (only available for the platforms listed below).

Platform	Option	Description
iOS	App Store ID	Optional. The App Store ID is required if you want to use the Apple App Store Volume Purchase Program (VPP) with your app. See also "Using the Apple App Store Volume Purchase Program (VPP)" on page 104.

Platform	Option	Description
Android	Is In Play Store	Select this check box if you want to import the app from Google Play.
Windows Phone	Generate random ID	Click this button to generate a random bundle ID.
Windows 8/RT	Generate random ID	Click this button to generate a random bundle ID.

Windows does not require a bundle ID which matches a certificate. But it is important that the ID has a certain format. You can create a random ID to make sure that the ID has the correct format.





- Click **Create App**.

Note: If you want to add screenshots, you have to edit the newly added app. See ["Editing an App" on page 65](#).


Displaying an App

After you have added a new app, you can check how it will appear in the app store. If you are not yet satisfied with the look of the new app, you can change it.

You can display an app via the following links which are provided at the top of the page:

Link	Description
 App Store	To display an app, you click its icon. The app is then shown as it would appear in your app store. It cannot be edited here. When you display an app in the app store and if you have the appropriate permission, a Manage App button is shown. When you click this button, you can immediately change the aspects of the app.
 Manage Apps	You can display an app in both views. In the list view () you click the app icon. In the grid view () you click the corresponding entry in the list. The app details are then shown, and you can view and change the aspects of the app.


Link	Description
	When you display an app, a Show in App Store button is shown. When you click this button, you can immediately view the app as it would appear in your app store.

When you display an app via the  **Manage Apps** link (or by clicking the **Manage App** button when you have displayed the app in the app store), the following navigation links are provided on the left side:

Link	Description
App Details	Shows the information that has been specified when this app has been added or last edited. You can use this page to edit, share, export or delete the app, or to view the log information. See "Managing the App Details" on page 63 for detailed information.
Versions	Shows the available versions of this app and the platforms for which the different versions are available, and allows you to add or delete versions. See "Managing the Versions of an App" on page 68 for detailed information.
Resources	Shows the available resource manifests for this app, and allows you to add or delete resource manifests. See "Managing the Resources of an App" on page 76 for further information.
Permissions	Shows the users who have permissions for this app. You can grant application-level permissions to users and user groups, or remove them. See "Managing the Permissions of an App" on page 83 for detailed information.
Build	Shows the available build configurations, build jobs and source code repositories for this app. You can add more build configurations and launch them, relaunch or delete build jobs, and define source code repositories. See "Managing the Builds of an App" on page 86 for detailed information.
Devices	Shows the devices on which the app has been installed, or - if the mobile device management has been allowed - the devices on which the app can remotely be installed, updated or removed. See "Managing the Devices on Which the App Can be Installed" on page 100 for detailed information.

Link	Description
Push	Allows you to send push notifications to the devices on which this app has been installed. See " Managing the Push Notifications for an App " on page 102 for detailed information.
VPP	The information shown on this page applies to the Apple App Store Volume Purchase Program (VPP). You can enter a redemption code which allows you to buy apps in volume through the VPP store and distribute them to your users. See " Using the Apple App Store Volume Purchase Program (VPP) " on page 104 for detailed information.
Analytics	Provides usage information on this app, including user reviews. This is useful as input for the optimization of your app. See " Viewing the App Analytics " on page 107 for detailed information.

Managing the App Details

When you display an app via the  [Manage Apps](#) link, the **App Details** page is shown first. You can use this page to edit, share, export, or delete the app, or to view the log information.

KarinDemo
Version 9.0 updated 2014-11-19
★★★★★

[Show in App Store](#)

Identifier	karindemo	Managed devices only	no
Category	Demo Applications	Downloads are public	no
Short Description	This is the short description		
Contact	Karin O.		
Copyright	No copyright information available		

Export Share Edit Log Delete

Platform information

Platform	ID	In vendor store
Android	com.softwareag.mobiledev.karindemo	✘
iOS	com.softwareag.mobiledev.karindemo	✘

Fully Compatible Devices
AOC Breeze, ASUS EeePadTransformerTF101, Acer IconiaTabA500, Acer LiquidA1, Acer LiquidE, Acer S100, Acer StreamS110, Alcatel OT980, Apple iPad (3rd Gen/CDMA), Apple iPad (3rd

The app icon and the information shown at the top (such as category, contact or managed devices only) has been specified when the app has been added or last edited.

The list under the heading **Platform information** shows the platforms (for example, Android or iOS) on which the app has been made available. It shows the bundle ID that has been defined when the app was added or last edited.

For your own apps for which you have the binaries, the **In vendor store** column shows an ✘. If you are viewing an app that has been added from a vendor store (for example, from Google Play), this column shows a checkmark (✓) and a **Pull Info from store-name** button. You can click this button to pull the metadata of the app from the vendor app store and thus update the information in your own app store.

✘ In vendor store

✓ [Pull Info from Play Store](#)

When you click and if this is one of your own apps for which you have the binaries, a dialog appears and you can immediately download the latest stable version (see also ["Downloading an Executable" on page 72](#)). If this is an app that you have added from a vendor store, the vendor store is invoked instead and the page for that app is shown. If the download icon is not shown for an entry, a version for this platform does not yet exist.


Under the heading **Fully Compatible Devices**, you can see the names of all devices that the app supports.

Editing an App

When you edit an app, you can change the information that is to be shown in the app store, such as the display name of the app, description, contact information, icon, screenshots or target-specific entries such as the bundle ID. Your changes will immediately be visible in the app store on the mobile device.

To edit the app details, you need the application-level permission **Edit Metadata** (see "[Overview of Application-Level Permissions](#)" on page 84) or the site-level permission **Manage Apps** (see "[Overview of Site-Level Permissions](#)" on page 141).

To edit an app

1. Click  **Manage Apps**.
2. Click the app that you want to edit.
3. On the **App Details** page, click **Edit**.
4. Make all required changes.

The options are the same as when adding a new app manually. See "[Specifying the Details for the New App Manually](#)" on page 58 for detailed information on the options.

5. If you want to add or change the icon, click **Browse** and select the icon from the resulting dialog box. When an icon has already been defined, "uploaded" is shown below the **Browse** button.
6. If you want to add one or more screenshots, do one of the following:
 - Click **Add Screenshot(s)** and select the screenshots from the resulting dialog box.
 - Drag the screenshots from your file system onto the edit page.

It may take a while until a screenshot will be shown on the edit page.



Note: Your screenshots can be viewed on all platforms. If your app runs on different platforms, keep this in mind when adding screenshots. For example, when your app runs on iOS and Android and you only add screenshots for Android, a user with an iOS device will also see them. Therefore, it is recommended that you remove the platform-specific elements from the screenshots or that you add a corresponding hint.

7. If you want to remove a screenshot, click the **Delete** button below that screenshot.
8. Click **Update App**.

Batch-Editing Several Apps

You can edit the details of several apps at the same time. For example, you can specify the same contact information or the same category for these apps.

To batch-edit several apps

1. Click  **Manage Apps**.
2. Make sure that the apps are shown in the list view ().
3. Select the check box for each app that you want to batch-edit.
4. Click **Batch Edit**.
5. Make all required changes.


You can edit the same options as shown when adding a new app manually, except for the identifier or icon. See "[Specifying the Details for the New App Manually](#)" on [page 58](#) for detailed information on the options.


6. Click **Update Apps**.

Sharing an App

You can share an app with other users. The user will receive an email with the information that the app is now available.

To share an app

1. Click  **Manage Apps**.
2. Click the app that you want to share.
3. On the **App Details** page, click **Share**.
4. On the resulting page, enter the user names, separated by a comma.


Tip: If you need more space for the email addresses, move the mouse pointer to the bottom right corner of the text box (). The mouse pointer changes and you can now resize the text box.

5. Click **Share**.

Exporting an App

You can export an app so that you can back it up or import it into a different Mobile Administrator instance (see also "[Importing an App](#)" on [page 56](#)). The exported app is a zip file which contains all metadata of the app and all of its versions.

To export an app

1. Click  **Manage Apps**.
2. Click the app that you want to export.
3. On the **App Details** page, click **Export**.

On the resulting page, you are informed that the export has been scheduled and that you will receive an email by the time the process is finished.


After a while, when the process has finished successfully, a **Download** button is shown.

4. Do one of the following:
 - Click **Download** to save the zip file to your disk.
 - If you want to download the file at a later point in time, click the download link in the mail that has been sent to you. Keep in mind that this link is only valid one day.

Viewing the Log Information for an App

When you view the log information for an app, you can see when and by whom this app has been created and updated.

To view the log information for an app

1. Click  [Manage Apps](#).
2. Click the app for which you want to view the log.
3. On the **App Details** page, click **Log**.

The **Maintenance** page is shown. When invoked via the app, the **Domain Log** tab of that page is filtered and shows only the entries related to the current app.

All other tabs of **Maintenance** page always provide information for the entire domain, not only for the current app. When you display one of these tabs and then return to the **Domain Log** tab, the logs for *all* changes in the domain will be shown. See ["Maintaining Mobile Administrator" on page 189](#) for more information on the different tabs of the **Maintenance** page.

Deleting an App

When you delete an app, it is no longer available in the app store.

You can delete an app from the **App Details** page of the app or from the list view of the **All Applications** page. In the list view, it is possible to delete several apps at the same time.

Tip: If you just want to hide an app from the app store listing, you need not delete it. You can just edit the app and set the corresponding option. See ["Editing an App" on page 65](#).

To delete an app

1. Click  [Manage Apps](#).
2. Do one of the following:

- Make sure that the apps are shown in the list view (☰) and then select the check box for each app that you want to delete.
 - Or, if you just want to delete a single app, click that app to display it. You can do this in both the list view and grid view.
3. Click **Delete**.
A dialog box appears, asking whether you are sure.
 4. Click **OK** to confirm the deletion.

Managing the Versions of an App

When you display an app, you can click the **Versions** link on the left side. If versions are already available for the app, they are listed on the resulting page. You can also add new versions from this page. If more than one version is available, the app store always offers for download the latest stable version.

Version	Product Stage	Platforms	Tags	Total Size	Crashes	Reviews	Created At
1.0/1234 5	none		bia		0	0	2014-08-28 15:40
0.0.2/3	Production (stable)	iOS		9.11 MB	0	0	2014-09-03 12:56
0.0.2/2	Production (stable)	iOS		9.11 MB	0	0	2014-09-03 12:44
0.0.2/1	Production (stable)	Android, iOS		9.26 MB	0	0	2014-08-25 15:14

Add Version from Executable

Browse... No file selected. Add Version

For each version, the list provides information such as the following:

- The product stage. This indicates whether a product is stable or unstable. See also ["Managing Product Stages" on page 167](#).
- The platforms for which this version has been built (for example, Android and/or iOS).
- How often this version has crashed.
- The number of reviews/comments from a vendor app store (such as Google Play or the Apple App Store).

You can click an app version to display detailed information on this version. You can then, for example, add or delete executables, view and edit the user comments or view the crash logs.

When the detailed information on an app is shown, you can edit the version (for example, to change the Release Notes text) or you can delete the version. When an app is currently unstable, a **Make Stable** button is provided. See also ["Making an App Version Stable"](#) on page 70.



Adding a New App Version

When you build your apps with Mobile Administrator, new app versions (executables) are created by the build jobs (see also ["Managing the Builds of an App"](#) on page 86). If you already have the binaries (for example, if you have imported apps or binary uploads), however, you have to create the app versions manually as described below.

To make a new app version available in the client app store, you first add a new version to your app. After that, you have to attach the executables to the app version. See ["Attaching an Executable to an App Version"](#) on page 71. When the executable has been attached, the new version will be visible on the mobile device. The user can then decide whether to install the latest stable or unstable version, if both versions exist and if the user has the permission to download unstable apps.

To add a new app version, you need the application-level permission **Manage Versions** (see ["Overview of Application-Level Permissions"](#) on page 84) or the site-level permission **Manage Apps** (see ["Overview of Site-Level Permissions"](#) on page 141).

To add a new app version

1. Click  **Manage Apps**.
2. Click the app for which you want to add a new version.
3. Click **Versions** on the left side.
4. Click .
5. Specify the following information:

Option	Description
Version number	Type version number.
Build number	Optional. Type the build number that is defined for the binary that you intend to attach.
Product stage	The product stage indicates whether a product is stable or unstable. Select the appropriate stage from the drop-down list box. See also "Managing Product Stages" on page 167.

Option	Description
Release notes	Optional. Type any text that is to be shown in the app store, in the section "What's New in Version <i>n</i> ".
Tags	Optional. Enter any tags, separated by a comma. The tags are used to determine the "Related Apps" that are shown when the user displays an app in the app store. They are also considered when searching the app store or when filtering the apps.
Created at	By default, the current date and time is shown. You can also select a different date and time using the corresponding drop-down list boxes.


6. Click **Create App Version**.

Editing an App Version

You can edit an app version, for example, if you want to add or modify the release notes for a version or if you want to specify additional tags.

To edit the release notes, you need the application-level permission **Manage Versions** (see ["Overview of Application-Level Permissions" on page 84](#)) or the site-level permission **Manage Apps** (see ["Overview of Site-Level Permissions" on page 141](#)).

To edit an app version

1. Click  **Manage Apps**.
2. Click the app for which you want to edit a version.
3. Click **Versions** on the left side.
4. In the list of versions, click the version that you want to edit.
5. Click **Edit**.
6. Make all required changes on the resulting page. This page provides the same options as when adding a version. See ["Adding a New App Version" on page 69](#).
7. Click **Update App Version**.


Making an App Version Stable

As long as the product stage of an app version is "unstable", a **Make Stable** button is shown on the details page of the app version.

To mark versions as stable or unstable, you need the application-level permission **Manage Versions** (see ["Overview of Application-Level Permissions" on page 84](#)) or the site-level permission **Manage Apps** (see ["Overview of Site-Level Permissions" on page 141](#)).

Note: You can also change the product stage by editing the app version. See ["Editing an App Version" on page 70](#).

To make an app version stable

1. Click  **Manage Apps**.
2. Click the app which has the version that you want to make stable.
3. Click **Versions** on the left side.
4. Click the version that you want to make stable
5. Click **Make Stable**.

Attaching an Executable to an App Version


This description applies if you already have the binaries, for example, if you have imported apps or binary uploads. In this case, it is not necessary that Mobile Administrator builds your apps (where the app versions are created by the build jobs).

After you have added an app version (see ["Adding a New App Version" on page 69](#)), you have to upload (attach) the executables (binaries). You can also attach executables to an existing version (for example, if the current app version can only be used on Android and you also want to make it available on iOS).

You can upload packaged mobile applications in the file formats listed in the section ["Installation and Prerequisites" on page 14](#), depending on the platform for which the version has been built.

To upload binaries, you need the application-level permission **Manage Versions** (see ["Overview of Application-Level Permissions" on page 84](#)) or the site-level permission **Manage Apps** (see ["Overview of Site-Level Permissions" on page 141](#)).

To attach an executable to an app version


1. Click  **Manage Apps**.
2. Click the app which contains the version to which you want to attach an executable.
3. Click **Versions** on the left side.
4. Click the version to which you want to add the executable.
5. On the **Executables** tab, which is shown at the bottom of the page, click **Browse** and select the executable from the resulting dialog box.
6. Click **Attach File** to upload the selected executable.

Adding a New App Version from an Executable

Instead of first adding an app version (see ["Adding a New App Version" on page 69](#)) and then attaching an executable (binary) to the version (see ["Attaching an Executable to an App Version" on page 71](#)), you can also do both at one go: You can directly create a new version of the app by uploading the application binary (see also the supported file formats listed in the section ["Installation and Prerequisites" on page 14](#)). The version number will be taken from the application bundle.

To upload binaries, you need the application-level permission **Manage Versions** (see ["Overview of Application-Level Permissions" on page 84](#)) or the site-level permission **Manage Apps** (see ["Overview of Site-Level Permissions" on page 141](#)).

To add an app from an executable

1. Click  **Manage Apps**.
2. Click the app for which you want to add a new version from an executable.
3. Click **Versions** on the left side.
4. Click **Browse** and select the executable from the resulting dialog box.
5. Click **Add Version**.



Downloading an Executable

You can download an executable from an app version. This is helpful, for example, if you want to upload the downloaded app to a vendor app store such as Google Play.

You can only download the executables of your own apps for which you have the binaries. It is not possible to download executables for apps that you have added from a vendor app store.

Note: You can also download the latest stable version directly from the **App Details** page. See ["Managing the App Details" on page 63](#).

To download an executable

1. Click  **Manage Apps**.
2. Click the app which contains the version from which you want to download an executable.
3. Click **Versions** on the left side.
4. In the list of versions, click the version from which you want to download an executable.
5. On the **Executables** tab, do one of the following:
 - Click  which is shown next to the entry for an executable.


- Or click the entry for an executable to display it and then click **Download**.

Deleting an Executable

You can delete an executable from an app version.

If this is the only executable of the version (for example, for iOS), the version can no longer be downloaded. However, if you have executables for all supported platforms and you delete the iOS executable, the Android and Windows versions can still be downloaded onto the mobile Android and Windows devices.


To delete an executable

1. Click  **Manage Apps**.
2. Click the app which contains the version from which you want to delete an executable.
3. Click **Versions** on the left side.
4. In the list of versions, click the version from which you want to delete an executable.
5. On the **Executables** tab, do one of the following:
 - Select the check boxes for the executables that you want to delete and click **Delete Selected**.
 - Or click the entry for an executable to display it and then click **Delete**.A dialog box appears, asking whether you are sure.
6. Click **OK** to confirm the deletion.

Displaying the Release Notes for an App Version

You can display the release notes text that has been specified for an app version. If you want to change the release notes, you have to edit the app version. See "[Editing an App Version](#)" on page 70.

To display the release notes

1. Click  **Manage Apps**.
2. Click the app which contains the version for which you want to display the release notes.
3. Click **Versions** on the left side.
4. In the list of versions, click the version for which you want to display the release notes.
5. Click the **Release Notes** tab.


Displaying the Build Jobs for an App Version

A build job is created when a build configuration is launched. See also ["Managing Build Jobs" on page 159](#).

When you display the build jobs, you can see when they have been created and updated and whether they were successful. You can delete build jobs, or you can click a build job to display its details.

You can either display the build jobs via the app version for which the jobs have been created (see below), via the **Build** page of the app (see ["Managing the Build Jobs of an App" on page 97](#)), or via the **All Build Jobs** page (see ["The All Build Jobs Page" on page 160](#)).

To display the build jobs for an app version

1. Click  **Manage Apps**.
2. Click the app which contains the version for which you want to display the build jobs.
3. Click **Versions** on the left side.
4. In the list of versions, click the version for which you want to display the build jobs.
5. Click the **Build Jobs** tab.
6. If you want to view the details for a build job, click the corresponding entry in the list. See also ["Displaying the Details of a Build Job" on page 161](#).
7. If you want to delete a build job, select the check box for this build job and click **Delete Selected**. See also ["Deleting a Build Job" on page 164](#).

Displaying the Crash Logs for an App Version


When the **Report app crashes** app policy has been defined in the build configuration of the app (see also ["Overview of App Policies" on page 88](#)), you can display a crash log when an app version crashes. Keep in mind that you have to create a separate build configuration for each platform on which you want to make the app available. See also ["Adding a Build Configuration" on page 91](#).

If you have created an app by uploading a binary, the **Report app crashes** app policy is automatically predefined.

Note: The crash will be reported the next time the app is started after the crash.

If you want to find out whether a crash has occurred for an app version, go to the **Versions** tab of the app and check the content of the **Crashes** column.

To display the crash logs for an app version

1. Click  **Manage Apps**.
2. Click the app which contains the version for which you want to display the crash logs.
3. Click **Versions** on the left side.
4. In the list of versions, click the version for which you want to display the crash logs.
5. Click the **Crash Logs** tab.
6. Click an entry in the list to display a crash group.

A list of individual crash logs is then shown. You can click each individual crash log to display further information. You can download a crash log, initialize crash log symbolication, or delete this individual crash log.


7. If you want to add a note to the crash group, click **Edit** (above the list of individual crashes). You can then specify a note and an abstract. Your note will be shown on the **Crash Logs** tab.
8. If you want to delete all crash logs in the crash group, click **Delete All Crash Logs** (above the list of individual crashes). Or click **Delete All Ignore** directly on the **Crash Logs** tab to delete all crash groups that are shown there.

Displaying the Comments for an App Version


You can display all comments that the users have written for an app version. You can add new comments, edit your own comments and delete comments.


It is not possible to display the comments for an app that has been pulled from a vendor store.

To display the comments for an app version

1. Click  **Manage Apps**.
2. Click the app which contains the version for which you want to display the comments.
3. Click **Versions** on the left side.
4. In the list of versions, click the version for which you want to display the comments.
5. Click the **Comments** tab.

This shows all comments, if available, one below the other.

6. To add a comment, click **Add Comment** and then enter your comment text.
7. To edit a comment that you have added yourself, click  which is shown to the right of the comment. It is not possible to edit the comments of other users.


8. If you want to delete a comment, click  which is shown to the right of the comment. You can delete the comments of any users. You will be asked whether you are sure.

Deleting an App Version

You can delete one or more app versions at the same time.

To delete an app version, you need the application-level permission **Manage Versions** (see "[Overview of Application-Level Permissions](#)" on page 84) or the site-level permission **Manage Apps** (see "[Overview of Site-Level Permissions](#)" on page 141).

To delete an app version

1. Click  **Manage Apps**.
2. Click the app for which you want to delete a version.
3. Click **Versions** on the left side.
4. Do one of the following:
 - Click the check boxes for the versions that you want to delete and click **Delete Selected**.
 - Or, if you just want to delete a single app version, click that version to display it and then click **Delete**.

A dialog box appears, asking whether you are sure.

5. Click **OK** to confirm the deletion.

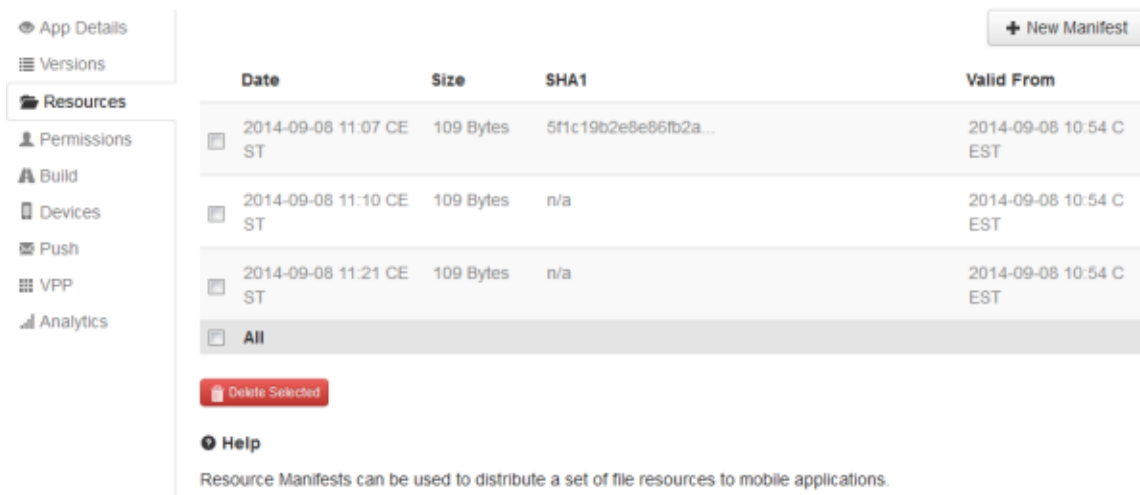
Managing the Resources of an App

A Mobile Administrator resource bundle contains a number of files (resources) that are provided to an app dynamically. A resource may be "bundled", that means, shipped as part of the app. Non-bundled resources or newer versions of bundled resources can be downloaded by the app at any time.

After creating and finalizing a manifest, download the bundle zip and extract its contents to get the file tree that should be included with the app.

The most current version of each resource is referenced by the SHA1 checksum in a resource manifest. A resource manifest describing the shipped version of the resource bundle is also shipped with the app. Updated versions of this manifest are downloaded by an app as they become available to identify updated resources.

When you display an app, you can click the **Resources** link on the left side. If resource manifests have already been set up for the app, they are listed on the resulting page.



Date	Size	SHA1	Valid From
2014-09-08 11:07 CE ST	109 Bytes	5f1c19b2e8e86fb2a...	2014-09-08 10:54 C EST
2014-09-08 11:10 CE ST	109 Bytes	n/a	2014-09-08 10:54 C EST
2014-09-08 11:21 CE ST	109 Bytes	n/a	2014-09-08 10:54 C EST
All			

Delete Selected

Help
Resource Manifests can be used to distribute a set of file resources to mobile applications.

If you want to make use of resource manifests, you have to

1. add a new resource manifest,
2. add resource files to the manifest,
3. finalize the resource manifest.

After a resource manifest has been finalized, the SHA1 value is shown in the list of manifests.

To create and upload resource manifests, you need the application-level permission **Manage Versions** (see "[Overview of Application-Level Permissions](#)" on page 84) or the site-level permission **Manage Apps** (see "[Overview of Site-Level Permissions](#)" on page 141).

Adding a New Resource Manifest

When you add a manifest, you can define the time from which the manifest will be valid. The current date and time is automatically provided, but you can also define a much later date and time. Keep in mind that you still have to add resource files to the manifest and that the manifest will only be available to your app on a mobile device after it has been finalized.

To add a manifest

1. Click **Manage Apps**.
2. Click the app to which you want to add a resource manifest.
3. Click **Resources** on the left side.
4. Click **New Manifest**.
5. Optional. On the resulting page, select the date and time (hour and minute) from which the manifest is valid.
6. Click **Create Manifest**.


The details page for the new manifest is shown. You can now add resources to the manifest. See "[Adding Resource Files to a Manifest](#)" on page 78.

Adding Resource Files to a Manifest

As long as a resource manifest has not been finalized, you can add resource files to the manifest. You add the resource files either by uploading single files manually or by batch-uploading files contained in a zip file.

By default, the resource files are bundled, that means, they are shipped as part of the app.

To add resource files to a manifest

1. Click  [Manage Apps](#).
2. Click the app to which you want to add resource files.
3. Click **Resources** on the left side.
4. Click an existing manifest to display the manifest details.
5. Do one of the following:
 - To upload a single file:
 - i. Click **New Resource**.
 - ii. Click **Browse** and then select the file that you want to upload.
The path and MIME type are automatically filled in.
 - iii. Deselect **bundled** if you do not want to bundle the resource.
 - iv. Click **Create Resource**.
 - To batch-upload files contained in a zip file:
 - i. Under the heading **Add/Replace Resources from ZIP**, click **Browse** and then select the zip file which contains the resources that you want to upload.
 - ii. Deselect **all bundled** if you do not want to bundle the resources.
 - iii. Click **Add Files**.

The uploaded resource files are shown under the heading **Resources**.

Deleting Resource Files from a Manifest

As long as a resource manifest has not been finalized, you can delete any files from the list of resource files.

To delete resource files from a resource manifest

1. Click  [Manage Apps](#).

2. Click the app for which you want to delete resource files.
3. Click **Resources** on the left side.
4. Click an existing manifest to display the manifest details.
5. Scroll down to the list of resource files.
6. Do one of the following:
 - Select the check box for each resource file that you want to delete and click **Delete Selected**.
 - Or click a resource file to display the details and then click **Delete**.A dialog box appears, asking whether you are sure.
7. Click **OK** to confirm the deletion.


Finalizing a Resource Manifest

As long as a resource manifest has not been finalized, a **Finalize Manifest** button is shown on the details page of the resource manifest. When you finalize a manifest, you make it available to the app on the mobile devices. You should do this after all resources have been added. The finalization creates a binary large object, where the name of the resulting file is *sha1-value*.blob.

When you finalize a manifest, it becomes available to the app either immediately or after the **Valid from** date. If you want to change this, you have to edit the manifest (see ["Changing the Availability Date of a Resource Manifest" on page 80](#)).

When a resource manifest has been finalized, it is no longer possible to add or delete resource files. If you want to do this, you have to duplicate the manifest (see ["Duplicating a Resource Manifest" on page 79](#)).


To finalize a resource manifest

1. Click  **Manage Apps**.
2. Click the app for which you want to finalize a resource manifest.
3. Click **Resources** on the left side.
4. Click the manifest to display the manifest details.
5. Click **Finalize Manifest**.

Duplicating a Resource Manifest

If you want to change the resource files in a manifest which has already been finalized, you have to duplicate the manifest. You can then add or delete resource files as required. When you finalize the duplicated manifest, it will take precedence over the old manifest and its contents will be distributed to the app on the mobile devices.

To duplicate a resource manifest

1. Click  [Manage Apps](#).
2. Click the app for which you want to duplicate a resource manifest.
3. Click **Resources** on the left side.
4. Click the manifest to display the manifest details.
5. Click **Duplicate Manifest**.


The details page for the duplicated manifest is shown.

6. Add or delete resource files as required.
7. Finalize the duplicated manifest to make it available.

Changing the Availability Date of a Resource Manifest

When you edit a resource manifest, you can define that the manifest is to be made available at a scheduled date and time.

To change the availability date of a resource manifest


1. Click  [Manage Apps](#).
2. Click the app for which you want to edit a resource manifest.
3. Click **Resources** on the left side.
4. Click the manifest to display the manifest details.
5. Click **Edit Manifest**.
6. Change the availability date and time on the resulting page.
7. Click **Update Manifest**.

Changing the Bundled Status of a Resource File

As long as a resource manifest has not been finalized, you can change the setting of a file's **bundled** option. In this case, an **Edit** button is shown when you view the details of the resource file.

The **bundled** option defines for each file whether the file needs to be available when the app is downloaded (bundled) or whether it is possible to download the file at a later point in time (not bundled).

To change the bundled status of a resource file



1. Click  [Manage Apps](#).
2. Click the app for which you want to edit a resource file.

3. Click **Resources** on the left side.
4. Click the manifest to display the manifest details.
5. Scroll down to the list of resource files.
6. Click a resource file to view its details.
7. Click **Edit**.
8. On the resulting page, click **bundled** to change the setting of this check box.
9. Click **Update Resource**.

Downloading a Single Resource File

You can download each resource file individually that has been added to a resource manifest. You can do this, for example, if you want to check the contents of this file.

To download a single resource file


1. Click  **Manage Apps**.
2. Click the app for which you want to download the resource file.
3. Click **Resources** on the left side.
4. Click the manifest to display the manifest details.
5. Scroll down to the list of resource files.
6. Click the  icon that is shown in front of the file name.

Downloading a Resource Manifest as a Human-Readable Zip File

You can download a resource manifest including all currently defined resource files as a zip file. This is helpful when creating a bundle. You can then check whether all required files are available.

You can always download the human-readable zip file, no matter whether the resource manifest has been finalized or not. The name of the resulting file is *app-name.zip*.


To download a resource manifest as a human-readable zip file

1. Click  **Manage Apps**.
2. Click the app for which you want to download the zip file.
3. Click **Resources** on the left side.
4. Click the manifest to display the manifest details.
5. Click **Human-Readable ZIP**.

Downloading a Resource Manifest as a Bundle Zip File

When a resource manifest has been finalized, the **Bundle ZIP** button is shown on the details page of the resource manifest. You can use this button to download the bundle that is delivered with the app. The name of the resulting file is BundledFiles.zip. The contents of this file is not human-readable.


To download a resource manifest as a bundle zip file

1. Click  [Manage Apps](#).
2. Click the app for which you want to download the zip file.
3. Click **Resources** on the left side.
4. Click the manifest to display the manifest details.
5. Click **Bundle ZIP**.

Downloading the Finalized Manifest as a Binary Large Object

When a resource manifest has been finalized, a link is shown on the details page of the resource manifest which allows you to download the binary large object (.blob) which has been created by the finalization.

To download the finalized manifest


1. Click  [Manage Apps](#).
2. Click the app for which you want to download the finalized manifest.
3. Click **Resources** on the left side.
4. Click the manifest to display the manifest details.
5. Click the link that is shown next to **SHA1** at the top of the details page.

Deleting a Resource Manifest

Older versions of a manifest are normally no longer required and can be deleted without any problems.

Caution: If you delete the current manifest, the app will no longer be able to download the resources.

To delete a resource manifest

1. Click  [Manage Apps](#).
2. Click the app for which you want to delete a resource manifest.

3. Click **Resources** on the left side.
4. Do one of the following:
 - Click the check boxes of the resource manifests that you want to delete and click **Delete Selected**.
 - Or click a manifest to display the manifest details and then click **Delete Manifest**.

A dialog box appears, asking whether you are sure.
5. Click **OK** to confirm the deletion.

Managing the Permissions of an App

When you display an app, you can click the **Permissions** link on the left side. The resulting page shows a list of all users who have permissions for the current app.

Name	View and Download Statistics	Download Unstable Versions	View Statistics	Edit Metadata	Manage Versions	Manage Resources	Manage Devices	Manage Builds	Manage User Permissions
admin	✓	✓	✓	✓	✓	✓	✓	✓	✓
buildnode	✓	✓	✓	✓	✓	✓	✓	✓	✓
jonas	✓	✓	✓	✓	✓	✓	✓	✓	✓
peter.nevermann	✓	✓	✓	✓	✓	✓	✓	✓	✓
tAdministrator	✓	✓	✓	✓	✓	✓	✓	✓	✓
tDeveloper	✓	✗	✗	✗	✗	✗	✗	✗	✗
tDeveloper	✓	✓	✓	✓	✓	✓	✓	✓	✓
thomas	✓	✓	✓	✓	✓	✓	✓	✓	✓
tiange.hu	✓	✓	✓	✓	✓	✓	✓	✓	✓
Training	✓	✗	✗	✗	✗	✗	✗	✗	✗

Show 10 entries

Remove Selected + Add User + Add User Group

The user entries are shown with different colors.

- **Black.** The entries for the users or user groups to whom application-level permissions have been granted are shown in black. If you are an administrator with the site-level permission **Manage Apps** or if you have been granted the application-level permission **Manage User Permissions** for this app, you can determine which permissions other users may have for the app. For example, you can define that a user can only edit the metadata of the app, or that a user may only view and download statistics. A

check box is provided for these users and user groups so that you can remove all application-level permissions for these users, if required.

- **Grey.** The entries for the users to whom the site-level permission **Manage Apps** has been granted are shown in grey. You cannot remove any application-level permissions for these users. Therefore, a check box is not shown for such a user.

See also "[Overview of Application-Level Permissions](#)" on page 84 and "[Overview of Site-Level Permissions](#)" on page 141.

Note: End-users normally only need the **View and Download Stable Versions** permission.

Overview of Application-Level Permissions

The application-level permissions are defined for an app. They are granted to individual users or user groups.

The following application-level permissions exist:

<u>Permissions</u>	<u>Description</u>
View and Download Stable Versions	May browse and download the application.
Download Unstable Versions	May download versions of this application which are not marked as stable.
View Statistics	May view and download this application's usage and download statistics and customer or user reviews.
Edit Metadata	May edit application metadata such as the application description, icon and screenshots, as well as platform-specific metadata like bundle or package IDs and vendor app store links.
Manage Versions	May add and remove versions of this application, upload binaries, edit version release notes and mark versions as stable or unstable.
Manage Resources	May create and update resource manifests used by this application.
Manage Devices	May trigger installation and removal of this app on managed devices.

Permissions	Description
Manage Build Jobs	May create and update build configurations, build jobs, source code repositories and provisioning profiles.
Manage User Permissions	May add and remove user permissions for this application.


Note: To assign permissions to other users, you need the site-level permission **Manage Apps** (see "[Overview of Site-Level Permissions](#)" on page 141) or the application-level permission **Manage User Permissions**.

Granting Application-Level Permissions to a User or User Group

If you want to grant permissions for a specific app to additional users or user groups, you have to add them to the list that is shown on the **Permissions** page of the app.

It may happen that a user has two different sets of permissions. For example, you add a user with many permissions to the app, and you also add a user group with less permissions to the app in which the same user is a member. In this case, the user will have all permissions as defined for the single user.


To grant application-level permissions to a user or user group

1. Click  **Manage Apps**.
2. Click the app for which you want to grant permissions.
3. Click **Permissions** on the left side.
4. **Add User** or **Add User Group**, depending on whether you want to grant permissions for a user or user group.
5. On the resulting page, select the user or user group.
6. Define the permissions as required.
7. Click **Add User** or **Add User Group**.

Editing the Application-Level Permissions of a User or User Group

You can change the application-level permissions for each user for whom a black entry is shown on the **Permissions** page of the app. These are the users who have been defined with the **Add User** and **Add User Group** buttons.

To edit the application-level permissions of a user or user group

1. Click  **Manage Apps**.
2. Click the app for which you want to edit the permissions.

3. Click **Permissions** on the left side.
4. Click the black entry for the user or user group for which you want to edit the application-level permissions.


Note: When you click a grey entry, you will see the user details in which the site-level permissions are defined. You cannot change the application-level permissions for such a user.

5. Change the application-level permissions as required.
6. Click **Update User** or **Update User Group**, depending on whether you are currently editing a user or user group.

Removing the Application-Level Permissions of a User or User Group

You can remove the application-level permissions for each user for whom a black entry is shown on the **Permissions** page of the app. These are the users who have been defined with the **Add User** and **Add User Group** buttons.

To remove the application-level permissions of a user or user group

1. Click  **Manage Apps**.
2. Click the app from which you want to remove the permissions.
3. Click **Permissions** on the left side.
4. Click the check boxes of the users or user groups for which you want to remove the permissions and click **Remove Selected**.

Note: This button is only shown if at least one user or user group with a blank entry is shown in the list.

A dialog box appears, asking whether you are sure.

5. Click **OK** to confirm the removal.

Managing the Builds of an App

When you display an app, you can click the **Build** link on the left side. The resulting page provides the following tabs:

Tab	Description
Build Configurations	Used to add build configurations for an app and to launch them. Launching a build configuration creates a build job. The result of a build job is a new version of the

Tab	Description
	app. See "Managing the Build Configurations of an App" on page 87.
Build Jobs	Used to view or relaunch the build jobs. See "Managing the Build Jobs of an App" on page 97.
Source Code Repositories	Used to load the source code for the build from a repository (instead of uploading it manually). See "Managing the Source Code Repositories of an App" on page 97.

To create and update build configuration, build jobs and source code repositories, you need the application-level permission **Manage Build Jobs** (see ["Overview of Application-Level Permissions"](#) on page 84) or the site-level permission **Manage Apps** (see ["Overview of Site-Level Permissions"](#) on page 141).

Managing the Build Configurations of an App

If build configurations have already been set up for the app, they are listed on the **Build Configurations** tab of the app. You only need build configurations for the apps that you want to build with Mobile Administrator on a remote build node. Build configurations are not required for apps that you import or add from a vendor store.

The screenshot displays the 'Build Configurations' tab in the Mobile Administrator interface. On the left, a sidebar contains navigation links: App Details, Versions, Resources, Permissions, Build (selected), Devices, Push, VPP, and Analytics. The main area shows a table with the following data:

ID	Platform	Repository	Product Stage	webMethods Mobile Designer	Tags
552	iOS	none	Production (stable)	IOS_Apple_Universal	
551	Android	none	Production (stable)	AND_generic_Android4xAPI	

Below the table, there are input fields for 'Version' (1.0), 'Build Number', and 'Source (ZIP)' with a 'Browse...' button. A 'Launch Selected Build Configs' button is located at the bottom of the configuration area.

You can create build configurations for your apps after the appropriate build nodes have been set up in your environment (see ["Managing Build Nodes"](#) on page 155). You need one build configuration for each platform (such as iOS or Android) on which you want to make your app available.

Besides the build node that is to be used, a build configuration defines, for example, the product stage (whether the product is stable or unstable), the app policies that are to be applied (for example, whether the app usage is to be logged) and whether notifications are to be sent to specific users when the build has finished (for example, in the case of a build failure).

When a build configuration for a platform has been created, you can launch it. This generates a build job for the platform. The build job will stay in the status "Running" for a while as the backend creates the source code for the app. When the build job is successful, the resulting version of the app will appear on the **Versions** page of the app.

If you have added an app for which you do not yet have ready-to-upload binaries, you can upload, for example, a project that has been created using Mobile Designer and you can then let Mobile Administrator build the target binaries remotely for you. The following steps are usually required in this case.

1. Create the app using the **I will enter the application details manually** link and define information such as the description, category, bundle ID, icon and screenshots. The app is not yet installable as no binaries have been provided yet. See also "[Specifying the Details for the New App Manually](#)" on page 58.
2. Grant the required permissions (for example, for a user group). See also "[Managing the Permissions of an App](#)" on page 83.
3. Create all required build configurations (for example, one for iOS and another one for Android). See "[Adding a Build Configuration](#)" on page 91.
4. Launch the build configurations in order to build the binaries. See "[Launching a Build Configuration](#)" on page 95.
5. Check the outcome of the build jobs. See "[Managing the Build Jobs of an App](#)" on page 97.
6. Access the app store client on your mobile device and make sure that the app is visible and installable. See "[Using the App Store on a Mobile Device](#)" on page 193.

Note: You can also run a remote build from Mobile Designer. See the Mobile Designer documentation for further information.

Overview of App Policies

App policies are defined when adding or editing a build configuration for an app. They are divided into enhancements and restrictions. They can be defined for iOS, Android and Windows Phone.

Enhancements

You can define the following enhancements for an app:

Policy	iOS	Android	Windows Phone	Description
Log app usage	X	X	X	If selected, information on the app usage is shown on the Usage and Downloads tab of the Analytics page of the app. See "Viewing the App Analytics" on page 107.
Monitor app usage	X			If selected, statistics are shown on the User Navigation tab of the Analytics page of the app. See "Viewing the App Analytics" on page 107.
Report app crashes	X	X	X	If selected, any app crashes are listed on the Crash Logs tab when you display an app version. See "Displaying the Crash Logs for an App Version" on page 74.
Register for push notifications	X			If selected, the app can send push notifications to the registered devices. See "Managing the Push Notifications for an App" on page 102.
Check for app updates	X			If selected, the installed app on the mobile device automatically checks whether an update (that is, a new app version) is available.
Force update	X			If selected, new app versions are automatically installed on the devices.

Restrictions

You can define the following restrictions for an app:

Policy	iOS	Android	Windows Phone	Description
Disable apps on jailbroken devices	X			If selected, the app cannot be installed on a jailbroken iOS device.
Require authentication to use the app	X			If selected, the user has to enter the Mobile Administrator credentials when starting the app on the mobile device.
Disable copy & paste within the app	X			If selected, it is not possible to copy and paste information within the app.
Disable file sharing via iTunes	X			If selected, the user cannot use this app to share data on iTunes.
App expires after date	X			If selected, the app can no longer be used after the date that you specify in the text box. When the user starts an app after it has expired, a message is shown indicating that the app has expired and that it can no longer be used.
Allow usage of this app only within the following radius	X		X	If selected, a text box is shown in which you can define the radius (in kilometers) within which the app can be used. In addition, a map is shown. Click or drag the marker in the map to set the starting point for the radius.



Adding a Build Configuration

When you add a build configuration - for example, for an app which runs on iOS - you can determine which version of the SDK on a build node is to be used to build the app, the provisioning profile that is to be used in the build, and the policies that are to be built into the app. Policies on iOS can disable copy and paste within the app or force authentication before the app can be used.

In addition to the app policies, you can also define the users who are to receive notifications in the case of successful or failed builds.

Note: When you add a build configuration, you have to specify a certificate for the platform to be used. If you have not yet uploaded the required certificate, see the appropriate section in ["Configuring Mobile Administrator" on page 27](#).

To add a build configuration

1. Click  **Manage Apps**.
2. Click the app for which you want to add a build configuration
3. Click **Build** on the left side.
4. On the **Build Configurations** tab, click .
5. Specify the following information:

Options	Description
Platform	Select the platform for which you want to create the build configuration (for example, iOS or Android).
Build node	Select the build node that is to be used. The drop-down list box provides for selection the build nodes that have already been set up. Defined build nodes that are currently not available are marked as "(offline)" in the drop-down list box. Make sure not to select an offline build node. When you select Auto-select , a build node will be used that meets the requirements (SDK, platform) for running the build job. See also "Managing Build Nodes" on page 155 .
Repository	Specify how the source code for the is to be made available. When a source code repository has been defined for the app (see "Adding a Source Code Repository" on page 98 , you can select the repository from this drop-down list box. The source code from that repository will then be used automatically when the build configuration is launched. When a source repository

Options	Description
	has not been defined for the app, it is only possible to select Source code will be uploaded manually . In this case, you have to upload a zip file containing the latest source code before launching the build configuration.
Product stage	Select the product stage. This can be either stable or unstable. See also " Managing Product Stages " on page 167.
Relative Source Path	Optional. Enter the relative path to the source code in the zip file that will be uploaded before the build configuration is launched. By default, the slash (/) is used.
Tags	Optional. Enter any tags, separated by a comma. The tags are used to determine the "Related Apps" that are shown when the user displays an app in the app store. They are also considered when searching the app store or when filtering the apps.
Scheduled?	Optional. Only shown when a source code repository has been defined for the app (see above). If selected, the build will automatically be started at the time defined in the Daily Schedule boxes (hour and minute).
Enable commit trigger	Optional. Only shown when a source code repository has been defined for the app (see above). If selected, the build is automatically started when a change is committed to the source code repository. This may occur in addition to the daily schedule.
Override app name	If selected, the app name as defined in the source code is used. If not selected (default), the app name as defined in the app details is used.
Override app icon	If selected, the app icon as defined in the source code is used. If not selected (default), the app icon as defined in the app details is used.
Run tests after build	If selected, all tests that are defined in the source code are run after the build job has finished.
Require tests to pass	If selected, a build job can only receive the status "Success" if all tests have run successfully. If not selected,

Options	Description
	a build job can receive the status "Success" even if one of the tests has failed.

The remaining options that are shown on this page pertain to the platform you have selected.

6. Specify the options for the selected platform.

- For iOS, specify the following:

Option	Description
iOS Provisioning Profile	Select a provisioning profile that you have previously uploaded. See also " Managing Provisioning Profiles " on page 175.
SDK Version	Select the SDK version that is to be used to build the app. You can select either Any to use the latest version on the build node or you can select a specific version number.
Xcode Schema Name	Optional. Enter the name of an Xcode scheme that is to be used to build the app.
Verbose output	If selected, verbose log output will be generated.

- For Android, specify the following:

Option	Description
Android Developer Certificate	Select a developer certificate that you have previously uploaded. See also " Managing Developer Certificates " on page 171.
API Level	Select the API level that is to be used. You can select either Any to use the latest level on the build node or you can select a specific level number.
Java Version	Select the Java version that is to be used to build the app. You can select either Any to use the latest version on the build node or you can select a specific version number.

- For Windows Phone and Windows 8/RT, specify the following:

Option	Description
Code Signing Certificate	Select a code signing certificate that you have previously uploaded. See also " Managing Developer Certificates " on page 171.
Main Project Name	Optional. Enter the name of the app project that is to be used to build the app.

Note: When you select a specific version instead of **Any**, this version must exist on the build node. Otherwise, you will find a hint in the details of the build job indicating that the build node does not support your selection.

- Optional. Under **webMethods Mobile Designer**, select **Build using webMethods Mobile Designer** if you want to build the app using the Mobile Designer SDK.

If selected, you have to specify the following additional options:

Option	Description
Target Name	Enter the "target device" as defined in Mobile Designer.
SDK Version	Specify the SDK version that is to be used to build the app. Or select Any to use the latest version on the build node.
Retain intermediate build files	Mobile Designer compiles native code in an intermediate step before launching the build. If selected, the files containing the native code are kept.

- Optional. Under **App Policies**, select the app policies that are to be applied. Only the policies which pertain to the selected platform are shown. See "[Overview of App Policies](#)" on page 88 for more information on the enhancements and restrictions that you can define.
- Optional. Under **Custom Build Parameters**, specify any parameters that your app requires. Specify the parameters in the following format:


```
key1=value1, key2=value2, ...
```

 Parameters will be made available as global project parameters (Mobile Designer builds) or precompiler definitions (iOS native builds).
- Optional. Under **Notification Settings**, click **Add User** if a user is to receive a notification after the app has been built. Select the user name from the resulting drop-down list, and then select the check boxes for the types of notifications that the user is to receive (for example, **on first failed build**).

If you want to remove a user that you have just added, click **Remove User** and select the user name from the resulting drop-down list.

Note: The changes to the list of users are only saved when you save all of your changes by clicking **Create Build Configuration**.


11. Click **Create Build Configuration**.

Launching a Build Configuration

When you launch a build configuration, you specify a version and build number. If you have not defined a source code repository in the build configuration, you have to select a zip file which contains the source code. A new build job is then generated which creates a new version of the app.

As long as you are testing your app and its build configuration, it is recommended that you define the product stage "unstable" in the build configuration. Otherwise, the new erroneous version of the app will immediately be available for download in your app store.

To launch a build configuration

1. Click  **Manage Apps**.
2. Click the app for which you want to launch a build configuration
3. Click **Build** on the left side.
4. On the **Build Configurations** tab, select the build configuration that you want to launch.
5. Specify the version number that you want to assign to the new version.
6. Optional. Specify the build number that you want to assign to the new version. If you do not specify a build number, it will automatically be incremented.
7. If you have not defined a source code repository in the build configuration, click **Browse** and then select the zip file which contains the source code.

The **Browse** button is not shown when a source code repository has been defined in the build configuration.

8. Click **Launch Selected Build Configs**.

A new build job is created. You can view it on the **Build Jobs** tab. The new version of the app will be shown on the **Versions** page of the app. Keep in mind that a new version may also be shown there when the build status is "Error" (for example, when the executables are still missing).


If users are to be notified, for example, when a new version is available or when the build has failed (see "[Adding a Build Configuration](#)" on page 91), the notifications are sent.

Note: If the build job results in the status "Error", you can view the errors and then relaunch the build job after the errors have been corrected. See also ["Managing Build Jobs" on page 159](#).

Editing a Build Configuration

You can edit a build configuration, for example, if you want to change an app policy or if you want to change the users who are to receive notifications in the case of failed or successful builds.

To edit a build configuration

1. Click  [Manage Apps](#).
2. Click the app for which you want to edit a build configuration.
3. Click **Build** on the left side.
4. On the **Build Configurations** tab, click the link for the configuration that you want to edit.
5. On the resulting page, click **Edit Build Configuration**.
6. Make all required changes.


For detailed information on the options, see ["Adding a Build Configuration" on page 91](#).

7. Click **Update Build Configuration**.

Duplicating a Build Configuration

You can create a build configuration by duplicating an existing build configuration.

To duplicate a build configuration


1. Click  [Manage Apps](#).
2. Click the app for which you want to duplicate a build configuration
3. Click **Build** on the left side.
4. On the **Build Configurations** tab, click the link for the configuration that you want to duplicate.
5. On the resulting page, click **Duplicate Build Configuration**.

The duplicated build configuration is immediately shown. If you want, you can now click **Edit Build Configuration** to edit the duplicated build configuration.

Removing a Build Configuration

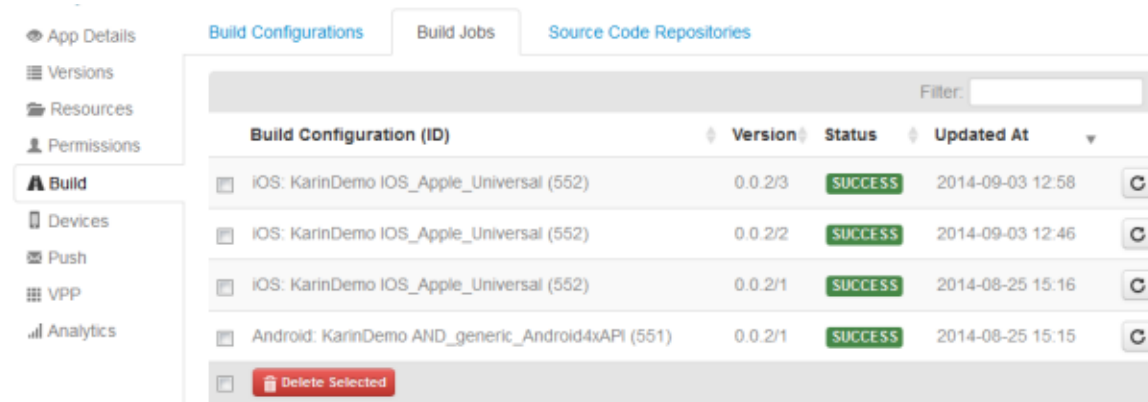
If a build configuration is no longer required, you can remove it.

To remove a build configuration

1. Click  **Manage Apps**.
2. Click the app from which you want to remove a build configuration
3. Click **Build** on the left side.
4. On the **Build Configurations** tab, click the link for the configuration that you want to remove.
5. On the resulting page, click **Remove Build Configuration**.
A dialog box appears, asking whether you are sure.
6. Click **OK** to confirm the removal.

Managing the Build Jobs of an App

A build job is created when you launch the build configuration for an app. The build jobs are listed on the **Build Jobs** tab of the app.



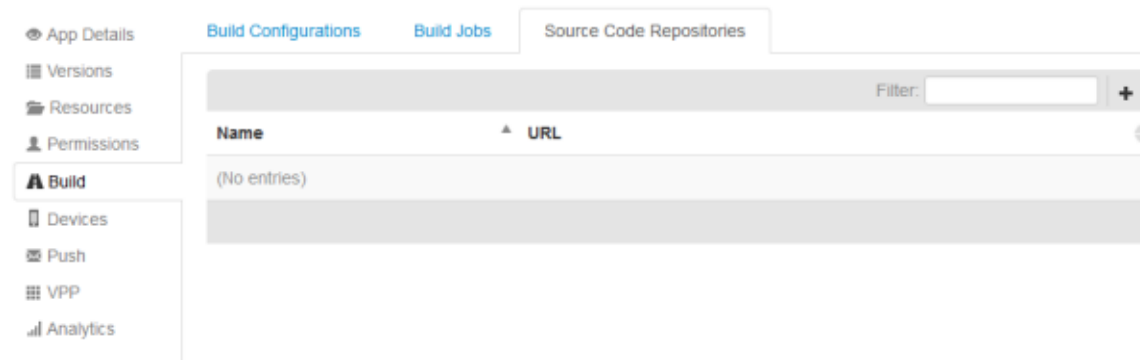
Build Configuration (ID)	Version	Status	Updated At
IOS: KarinDemo IOS_Apple_Universal (552)	0.0.2/3	SUCCESS	2014-09-03 12:58
IOS: KarinDemo IOS_Apple_Universal (552)	0.0.2/2	SUCCESS	2014-09-03 12:46
IOS: KarinDemo IOS_Apple_Universal (552)	0.0.2/1	SUCCESS	2014-08-25 15:16
Android: KarinDemo AND_generic_Android4xAPI (551)	0.0.2/1	SUCCESS	2014-08-25 15:15

You can relaunch or delete build jobs. When you display a build job, you can display the console output for the build job or any errors that may have occurred. For detailed information, see ["Managing Build Jobs" on page 159](#).

Managing the Source Code Repositories of an App

When you define a source code repository for an app, you can automatically load the source code for the app from that repository. If you want to do this, you also have to define the repository in the build configuration. See ["Adding a Build Configuration" on page 91](#).

If source code repositories have been defined, they are listed on the **Source Code Repositories** tab of the app. You can define one or more source code repositories, and you can remove them.



Adding a Source Code Repository

When you add a source code repository to the **Build** page of an app, you can select it when adding a build configuration for that app. See also "[Adding a Build Configuration](#)" on page 91. Thus, you need not upload the source code manually.

To add a source code repository

1. Click **Manage Apps**.
2. Click the app for which you want to add a source code repository.
3. Click **Build** on the left side.
4. Click the **Source Code Repository** tab.
5. Click **+**.
6. Specify the following information:

Option	Description
Title	The name of the current app is automatically provided. The title is shown on the Source Code Repository tab. If you have more than one source code directory, you can specify a different title for each repository entry.
Type	Select the type of your source code repository: Git or SVN.
URL	The URL to your source code repository.
Username	Optional. A user name for logging in to the repository.
Password	Optional. The password of the above user.
SSH Private Key	If you want to use SSH key authentication, user name and password must be left empty. Specify a valid private key that has access to the repository.


Option	Description
Branch	Git only. The name of the branch that you want to build.

7. Click **Create Repository**.

Editing a Source Code Repository

If you need to change the information that has been defined for a source code repository, you can edit it.


To edit a source code repository

1. Click  **Manage Apps**.
2. Click the app for which you want to edit a source code repository.
3. Click **Build** on the left side.
4. Click the **Source Code Repository** tab.
5. Click the entry for the source code repository that you want to edit.
6. Click **Edit Repository**.
7. On the resulting page, change the required information. For detailed information on the available options, see "[Adding a Source Code Repository](#)" on page 98.
8. Click **Update Repository**.

Removing a Source Code Repository

If the definition of a source code repository is no longer required for an app, you can remove it.

To remove a source code repository

1. Click  **Manage Apps**.
2. Click the app for which you want to remove a source code repository.
3. Click **Build** on the left side.
4. Click the **Source Code Repository** tab.
5. Click the entry for the source code repository that you want to remove.
6. Click **Remove Repository**.
A dialog box appears, asking whether you are sure.
7. Click **OK** to confirm the removal.

Managing the Devices on Which the App Can be Installed

When you display an app, you can click the **Devices** link on the left side. The list on the resulting page is filled automatically.

User	Device	Status	Version	Latest
andreas	iPhone 5s	Installed	1.0/75	no
andreas	iPod touch (5th Gen)	Installed	1.0/76	no
<input type="checkbox"/> andreas	HTC One	Managed	1.0/77	yes

The list shows the devices on which the app has been installed, or - if the mobile device management has been allowed - all managed devices on which the app can remotely be installed, updated or removed.

- **Managed Devices.** A check box is shown for each device on which the mobile device management has been allowed. You can remotely install and update the app on a managed device, and you can also remotely remove the app from a managed device. To trigger these actions, you need the application-level permission **Manage Versions** (see "[Overview of Application-Level Permissions](#)" on page 84) or the site-level permission **Manage Apps** (see "[Overview of Site-Level Permissions](#)" on page 141).
- **All Other Devices.** When the mobile device management has not been allowed on a device, the app can only be installed directly on the device, by downloading it from the app store. A check box is not shown for such a device.

The **Status** column provides the following information:

- **Not installed.** The device is managed, but app has not been installed on that device.
- **Managed.** The device is managed, and the app has been installed on that device.
- **Installed.** The device is not managed, and the app has been installed on that device.


You can click a device to display more information on that device (for example, if you want to check the iOS or Android version that is installed on the device or if you want to see which other apps are installed on the device), or to manage the device (for example, to lock the device if the device management has been allowed).

If you want to display all devices that have been registered in Mobile Administrator, click the **Devices** link that is shown at the top of the page. For more information, see "[Managing Devices](#)" on page 109.

Installing an App on a Managed Device

You can remotely install an app on the devices on which the user has allowed the mobile device management. Depending on the platform, this installation is either automatically performed on the mobile device without user interaction (iOS) or the user is asked to confirm the installation (Android).


To install an app on a managed device

1. Click  **Manage Apps**.
2. Click the app that you want to install.
3. Click **Devices** on the left side.
4. Select the check boxes for the devices on which you want to install the app.
5. Click **Install**.
A dialog box appears, asking whether you are sure.
6. Click **OK** to confirm the installation.

Updating an App on a Managed Device

You can remotely update an app on the devices on which a previous version has already been installed. The most recent stable version of the app will then be installed. Depending on the platform, this update is either automatically performed on the mobile device without user interaction (iOS) or the user is asked to confirm the update (Android).


To update an app on a managed device

1. Click  **Manage Apps**.
2. Click the app that you want to update.
3. Click **Devices** on the left side.
4. Select the check boxes for the devices on which you want to update the app.
5. Click **Update**.

Removing an App from a Managed Device

You can remotely remove an app from the devices on which it has been installed. Depending on the platform, this removal is either automatically performed on the mobile device without user interaction (iOS) or the user is asked to confirm the removal (Android).

To remove an app from a managed device

1. Click  [Manage Apps](#).
2. Click the app that you want to remove.
3. Click **Devices** on the left side.
4. Select the check boxes for the devices from which you want to remove the app.
5. Click **Remove**.

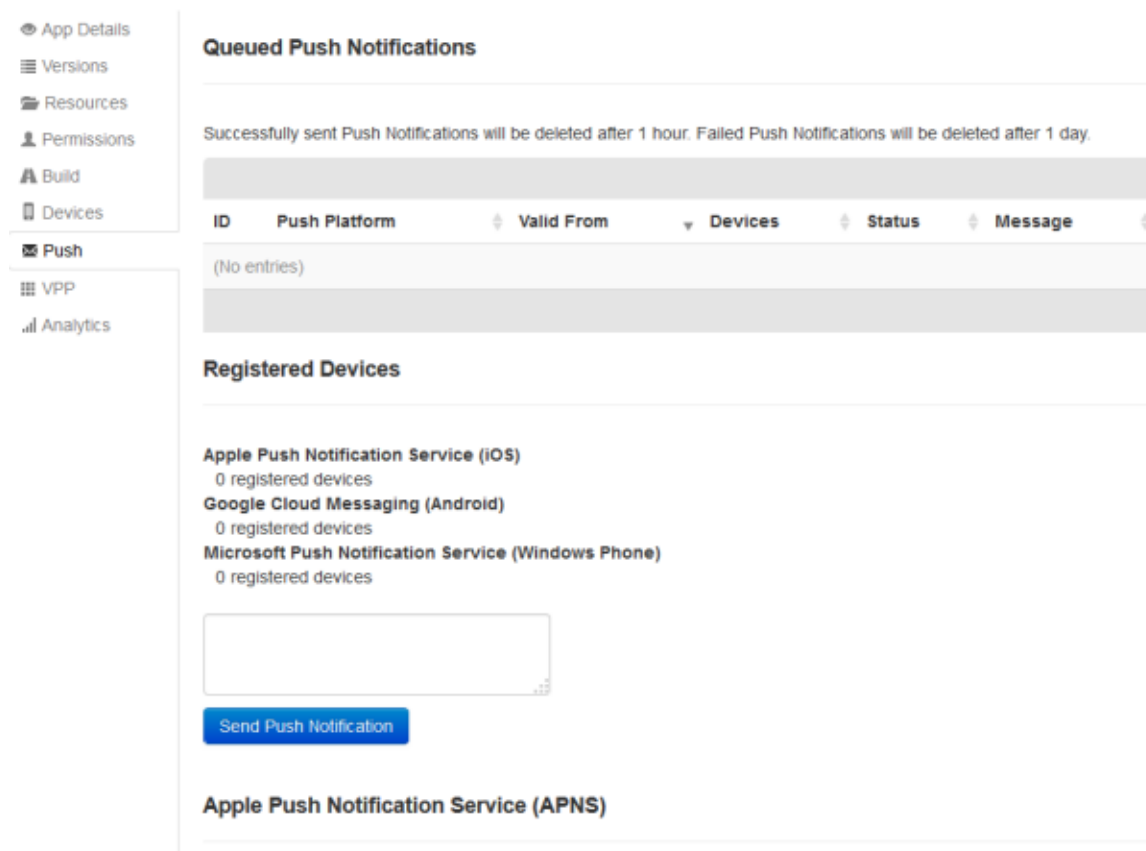
A dialog box appears, asking whether you are sure.

6. Click **OK** to confirm the removal.

Managing the Push Notifications for an App

When you display an app, you can click the **Push** link on the left side. The resulting page allows you to send push notifications to all devices on which the app has been installed. These devices are also called "registered devices".

The prerequisite for sending push notifications is that the app has been programmed to support push notifications. For iOS apps, this can easily be set with the app policy **Register for push notifications**. See also "[Overview of App Policies](#)" on page 88.



The screenshot shows the 'Push' section of the app management interface. On the left is a navigation menu with options: App Details, Versions, Resources, Permissions, Build, Devices, Push (selected), VPP, and Analytics. The main content area is titled 'Queued Push Notifications' and includes a table with columns: ID, Push Platform, Valid From, Devices, Status, and Message. Below the table, it shows '(No entries)'. Underneath is the 'Registered Devices' section, which lists three services: Apple Push Notification Service (iOS) with 0 registered devices, Google Cloud Messaging (Android) with 0 registered devices, and Microsoft Push Notification Service (Windows Phone) with 0 registered devices. There is a text input field and a 'Send Push Notification' button. At the bottom, the 'Apple Push Notification Service (APNS)' section is partially visible.

Additional prerequisites for sending push notifications are the following (this can be specified at the bottom of the page):

- A production and/or development certificate for the Apple Push Notification Service (APNS). See also "[Adding Certificates for the Apple Push Notification Service \(APNS\)](#)" on page 103.
- An API key for Google Cloud Messaging (GCM). See also "[Specifying an API Key for Google Cloud Messaging \(GCM\)](#)" on page 104.

There are no such requirements for the Microsoft Push Notification Service (MPNS).


If a push notification has recently been sent, a corresponding entry is shown in the list of queued push notifications. The **Valid From** column indicates when a push notification has been sent. When a push notification has been sent successfully (status "Success"), it will be deleted from the list after 1 hour. If a push notification could not be sent (status "Unsent"), it will be deleted from the list after 1 day. This may happen, for example, if an invalid token was specified or if the service could not be reached.

The **Push Platform** column indicates to which service the push notification has been sent. This can be "APNS", "GCM", "MPNS", or "Multiple" if the push notification has been sent to more than one service.

Adding Certificates for the Apple Push Notification Service (APNS)

If you want to be able to send push notifications for an app to an iOS device, you have to add a push certificate for production mode to that app. In addition, you can also add a push certificate for development mode - this is helpful if you are still testing an app which has not yet been made available in the app store.


To add a push certificate

1. Click  [Manage Apps](#).
2. Click the app for which you want to add a push certificate.
3. Click **Push** on the left side.
4. Scroll down and click either **Add Certificate (Production)** or **Add Certificate (Development)**.
5. Click **Certificate Signing Request** and then download the certificate signing request.
6. Click the link for the **iOS Provisioning Portal** and then proceed as follows:
 - a. Sign in with your Apple ID.
 - b. Configure the App ID for your app.
 - c. Activate the Production Push Notification service using the certificate signing request that you have downloaded.
7. Click **Browse** and select the push certificate that you have downloaded from the iOS Provisioning Portal.
8. Click **Upload Certificate**.

Specifying an API Key for Google Cloud Messaging (GCM)

If you want to be able to send push notifications for an app to an Android device, you have to specify an API key for Google Cloud Messaging (GCM) for that app. You need a separate key for each app. For more information on how to obtain such a key, see <http://developer.android.com/google/gcm/gs.html>.


To specify the API key for Google Cloud Messaging


1. Click  **Manage Apps**.
2. Click the app for which you want to add the API key.
3. Click **Push** on the left side.
4. Scroll down and enter the key in the **GCM API Key** text box.
5. Click **Save**.

Sending a Push Notification

You can send push notifications to all registered devices, that is, to all devices on which the app has been installed.

To send a push notification

1. Click  **Manage Apps**.
2. Click the app for which you want to send a push notification.
3. Click **Push** on the left side.
4. Scroll down and enter your notification text in the text box.

Tip: If you need more space for your notification text, move the mouse pointer to the bottom right corner of the text box (). The mouse pointer changes and you can now resize the text box.

5. Click **Send Push Notification**.

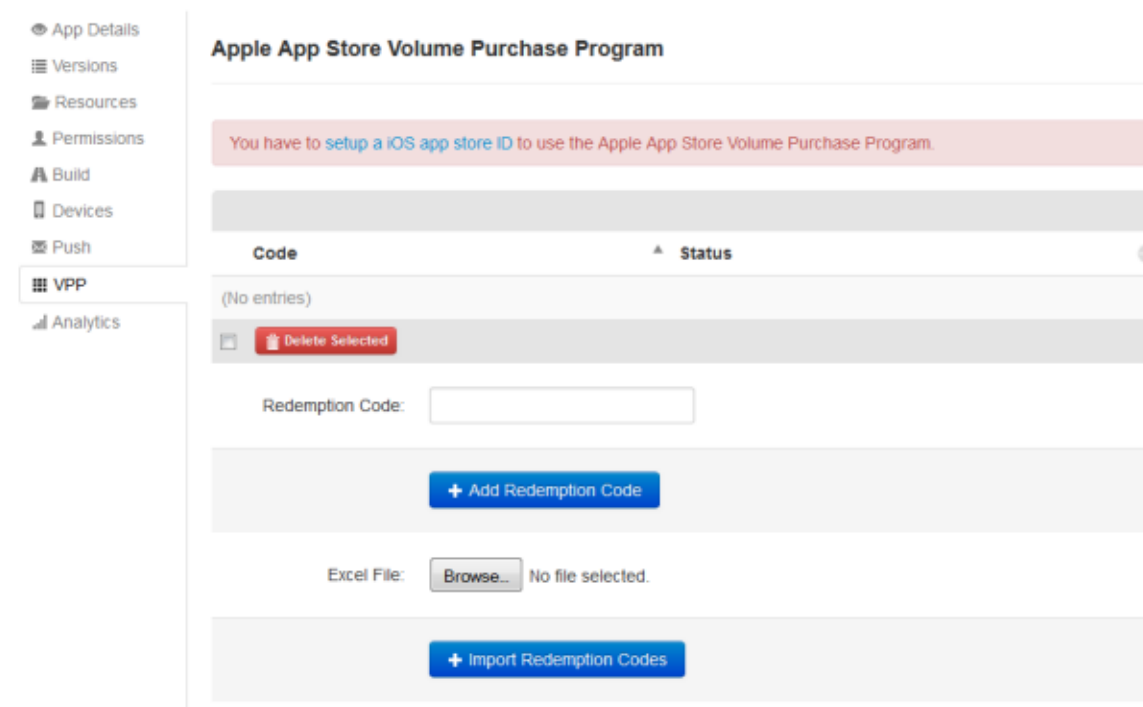
An entry for the new push notification is now shown in the list of queued push notifications.

Using the Apple App Store Volume Purchase Program (VPP)

When you display an app, you can click the **VPP** link on the left side. The resulting page allows you to add or import redemption codes for Apple's Volume Purchase Program (VPP). When you enroll in this program, you receive a redemption code which allows you to buy apps in volume from the VPP store and distribute them to your users.

For example, if your users need the paid app XYZ from the App Store, your company can buy this app, for example, 1000 times. You can then make this app available in Mobile Administrator (see also ["Adding an App from a Vendor App Store" on page 57](#)) so that your users do not have to pay for it.

To use the Apple App Store Volume Purchase Program with an app, you have to set up an iOS app store ID for that app. See also ["Editing an App" on page 65](#).



Apple delivers the redemption codes in a spreadsheet (Excel file). A unique code is provided for each app in the quantity purchased. For example, if you buy an app 1000 times, you will receive 1000 different redemption codes.

You can add the redemption codes to Mobile Administrator in two ways: by entering each redemption code in the text box or by importing multiple redemption codes from the spreadsheet.


The spreadsheet also includes a redemption URL with the redemption code embedded in the link. It is recommended that you send the redemption URL to your users, so that they do not have to enter the redemption code manually when downloading the app.

Each time the app is downloaded, the **VPP** page in Mobile Administrator is updated so that the number of redeemed codes can be tracked at any time.

Adding a Single Redemption Code

You can add single redemption codes to the app. Repeat the procedure below for each redemption code that you have received for the app.


To add a redemption code

1. Click  **Manage Apps**.
2. Click the app for which you want to add the redemption code.
3. Click **VPP** on the left side.
4. Type in or paste the redemption code in the corresponding text box.
5. Click **Add Redemption Code**.

Importing Multiple Redemption Codes

You can import multiple redemption codes from an Excel file.


To import multiple redemption codes

1. Click  **Manage Apps**.
2. Click the app for which you want to import the redemption codes.
3. Click **VPP** on the left side.
4. Click **Browse** and select the required file.
5. Click **Import Redemption Codes**.

Deleting a Redemption Code

You can delete a redemption code, for example, if you have entered the wrong code in the text box.

To delete a redemption code

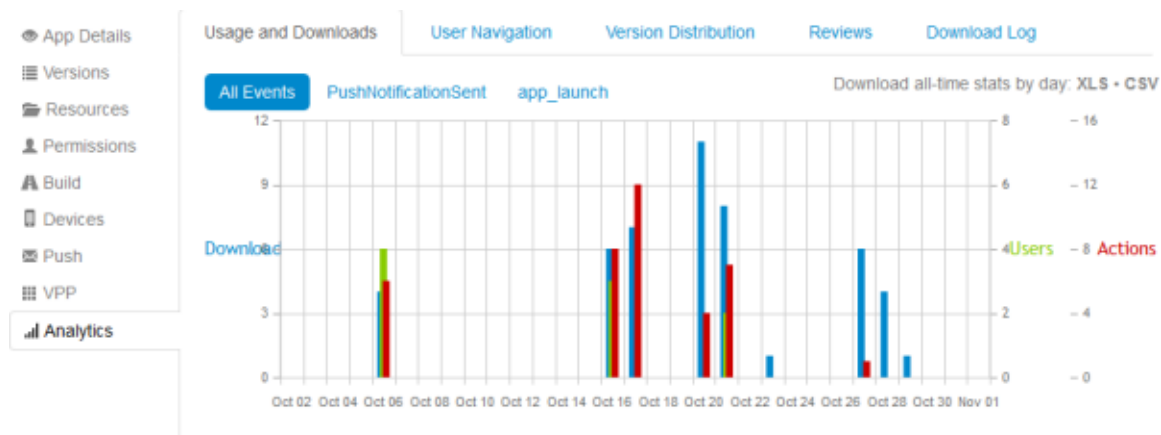
1. Click  **Manage Apps**.
2. Click the app from which you want to delete the redemption code.
3. Click **VPP** on the left side.
4. Select the check box for each redemption code that you want to delete.
5. Click **Delete Selected**.

A dialog box appears, asking whether you are sure.

6. Click **OK** to confirm the deletion.

Viewing the App Analytics

Mobile Administrator captures usage information on an app either directly or by pulling it from the enterprise app store, including user reviews. This is useful as input for the optimization of your apps.



When you display an app, you can click the **Analytics** link on the left side. The resulting page provides the following tabs which provide statistics on app usage and downloads:

- **Usage and Downloads.** This tab shows a graph for the last 31 days (including the current day) indicating the number of downloads on each day. The usage information is the result of the **Log app usage** app policy which is defined in the build configuration. See also "[Overview of App Policies](#)" on page 88.

Different events may be shown. You can view each event separately by clicking the corresponding link above the graph. Clicking **All Events** always shows all types of events.

You can save the currently shown statistics information in Excel (XLS) or CSV format. The resulting file shows the number of downloads by day.

The downloads are shown for all apps in your app store, including those that you have added from a vendor app store. All other tabs only show information for your own apps.

- **User Navigation.** This tab shows which pages the users have invoked inside the app and provides statistics on these pages (such as number of sessions and page visits, average usage time). This information is the result of the **Monitor app usage** app policy which is defined in the build configuration (iOS only). See also "[Overview of App Policies](#)" on page 88.
- **Version Distribution.** This tab shows which versions of the app have been in use during the last 24 hours.
- **Reviews.** This tab shows the user reviews and comments that have been given for this app in both your own app store and in the Apple App Store.

- **Download Log.** This tab lists all users who have downloaded the app on a certain date, regardless of whether the app is still installed on their devices.

Note: If you want to view the devices on which the app is currently installed, go to the **Devices** page of the app. See ["Managing the Devices on Which the App Can be Installed"](#) on page 100.

To view the app analytics, you need the application-level permission **View Statistics** (see ["Overview of Application-Level Permissions"](#) on page 84) or the site-level permission **Manage Apps** (see ["Overview of Site-Level Permissions"](#) on page 141).

4 Managing Devices


■ Overview	110
■ The All Devices Page	110
■ Organizing Devices in Groups	111
■ Managing a Device	114

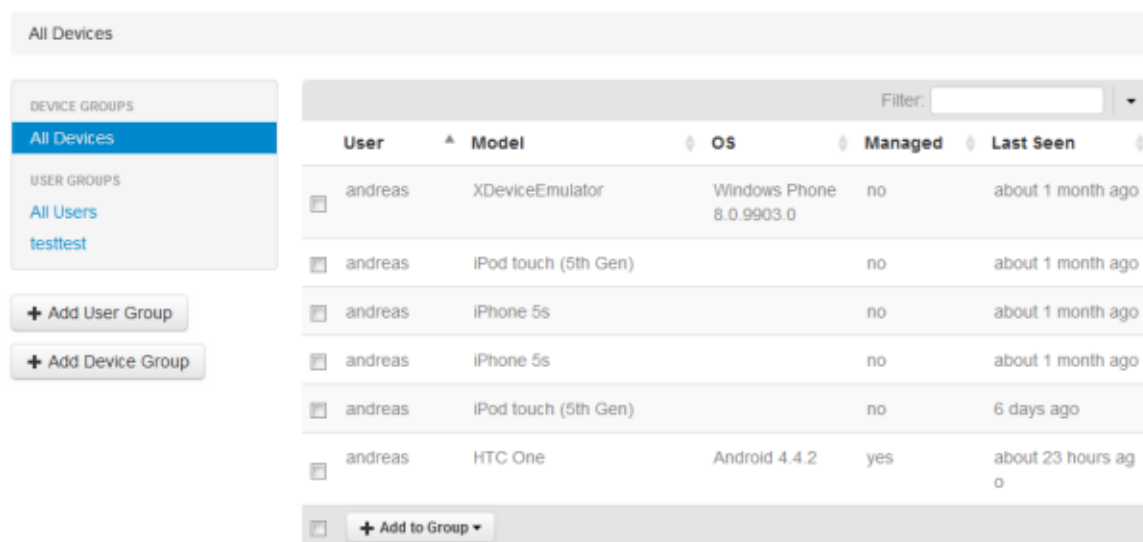
Overview

A device is automatically registered in Mobile Administrator when your app store client is installed on that device and the device owner has logged in with the correct credentials. You can organize the registered devices in groups, and you can assign existing device policies to these groups. See ["Policy Types" on page 125](#) for an overview of the policies that can be defined. You can manage a registered device remotely when the mobile device management has been allowed on this device. It is then possible, for example, to remotely lock or wipe a device, which is very helpful when a device was lost or stolen.

To organize and manage the devices of other users, you need the site-level permissions **Manage Devices** and **Wipe Devices**. To assign device policies to devices, you need the site-level permission **Assign Policies**. See also ["Overview of Site-Level Permissions" on page 141](#). These site-level permissions are not required if users want to remotely manage their own devices. When the mobile device management has been allowed on the device, each user can, for example, remotely lock or wipe the own device.

The All Devices Page

When you click  **Devices**, the **All Devices** page is shown which lists all mobile devices which have been registered in Mobile Administrator, along with the name of the user who owns that device. The **Managed** column indicates whether the mobile device management has been allowed on the device; when this has been done, "yes" is shown. The information in the **Last Seen** column indicates when your app store client was last accessed with that device.



The screenshot shows the 'All Devices' page. On the left, there is a sidebar with 'DEVICE GROUPS' (All Devices) and 'USER GROUPS' (All Users, testtest). Below the sidebar are buttons for '+ Add User Group' and '+ Add Device Group'. The main area is a table with a filter input and columns: User, Model, OS, Managed, and Last Seen. The table contains six rows of device data.

User	Model	OS	Managed	Last Seen
andreas	XDeviceEmulator	Windows Phone 8.0.9903.0	no	about 1 month ago
andreas	iPod touch (5th Gen)		no	about 1 month ago
andreas	iPhone 5s		no	about 1 month ago
andreas	iPhone 5s		no	about 1 month ago
andreas	iPod touch (5th Gen)		no	6 days ago
andreas	HTC One	Android 4.4.2	yes	about 23 hours ago

At the bottom of the table is a '+ Add to Group' button.

Tip: You can also access this page from the dashboard: In the **Domain Information** box, click the number that is shown next to **Managed Devices**. Or click the header of the **Managed Devices** box.

Using this page, you can add new groups with different policies in which you organize your devices, and you can delete groups. Apart from the groups, you can also display information on single devices and, if the mobile device management has been allowed on a device, you can remotely manage this device.

Using the **Filter** box, you can restrict the list to show only those items that meet your filter criteria. For example, you can restrict the list to a specific operating system, user name, or model. Or you can enter "yes" (as shown in the **Managed** column) to display only the devices on which the mobile device management has been allowed. See also "[Filtering Lists](#)" on page 22.

The left side of the page shows the device groups and user groups that have already been defined.


Organizing Devices in Groups

You can define device groups and user groups. For each of these groups, you can define different policies (see also "[Managing Policies](#)" on page 121). The policies will then be applied to the devices defined in the group. For example, you can define a device group where the devices cannot be used to take photos. Or you can define a user group that is allowed to use a specific WiFi network.

Adding a User Group as a Device Group

You can make an existing user group available as a device group. This is helpful, if you want to assign the same set of policies to all devices that are used by the members of the user group. See also "[Creating a Local User Group](#)" on page 152.

To add a user group as a device group


1. Click  **Devices**.
2. Click **Add User Group**.
3. On the resulting page, select the user group that you want to add as a device group from the drop-down list box.
4. Click **Add User Group**.

The name of the selected group is shown on the left side of the **All Devices** page, under the heading **USER GROUPS**. You can now define the policies for the new group. See "[Adding a Policy to a Group](#)" on page 112.

Adding a Device Group

You can add an empty device group and then define all devices that are to belong to that device group. For example, you can create a device group for the devices used by external employees and another device group for the employees who have customer contacts. You can then define different policies for these device groups. Keep in mind that a user may have more than one device.

To add a device group


1. Click  **Devices**.
2. Click **Add Device Group**.
3. On the resulting page, enter a name for the new device group.
4. Click **Create Device Group**.

The name of the new device group is shown on the left side of the resulting page, and its contents (which is currently empty) is shown on the right. You can now define the policies that are to be applied to the devices that you still have to define for the new group. See also ["Adding a Policy to a Group" on page 112](#) and ["Adding a Device to a Device Group" on page 113](#).

Adding a Policy to a Group

When you add a policy to a group, it is applied to all devices that have been added to that group. You can add policies to all groups (device groups and user groups) that are listed on the **All Devices** page, including the user group "All Users". There is one exception: it is not possible to define policies for the device group "All Devices".

To add a policy to a group

1. Click  **Devices**.
2. On the left side of the resulting page, click the name of the device group or user group.
3. Go to the bottom of the page and select the policy from the drop-down list box.
4. Click **Add Policy**.


An entry for the new policy is now shown under the heading **Group Policies**.

Caution: If you click the newly added policy to display it and then click **Edit Policy**, you do not only edit the policy for the current group. You will edit this policy for all devices to which is policy is applied. See also ["Editing a Device Policy" on page 124](#).

Removing a Policy from a Group

You can remove policies from any device groups and user groups, including the user group "All Users". Keep in mind that it is not possible to define policies for the device group "All Devices"; therefore it is not possible to remove policies from this group.

To remove a policy from a group


1. Click  **Devices**.
2. On the left side of the resulting page, click the name of the device group or user group.
3. Go to the bottom of the page and select the check boxes for the policies that you want to remove.
4. Click **Remove Selected Policies**.
A dialog box appears, asking whether you are sure.
5. Click **OK** to confirm the removal.

Caution: If you click the policy name to display the policy and then click **Delete Policy**, you do not only remove the policy from the group. You delete this policy altogether so that it can no longer be assigned to any device. See also ["Deleting a Device Policy" on page 124](#).

Adding a Device to a Device Group

You can add a device to one or more device groups. The policies defined for these device groups are then applied to the device.


To add a device to a device group

1. Click  **Devices**.
2. Select the check box for each device that you want to add to a group.
You can do this in the list of all devices or in the list of all users. If the device has already been assigned to a group, you can also display the devices in a specific device group or user group and then select the check box for that device.
3. Click **Add to Group** and select the name of the device group from the drop-down list.

Removing a Device from a Device Group

You can remove a device from a device group, for example, if the policies defined for that device group should no longer be applied to the device.

To remove a device to a device group

1. Click  [Devices](#).
2. On the left side of the resulting page, click the name of the device group
3. Select the check box for each device that you want to remove from the group.
4. Click **Remove From Group**.

The selected devices are immediately removed from the group. You are not asked whether you are sure.

Caution: If you click the **Delete** button instead, you will delete the device from Mobile Administrator. See also "[Removing a Device](#)" on page 120.


Deleting a Device Group

You can delete all device groups that have been added. This does not delete the devices. But it removes the policies that have been defined for the devices in this device group.


The device group "All Devices" cannot be deleted.

User groups cannot be deleted from the **All Devices** page. If you want to delete a user group, go to the **All User Groups** page. See "[Deleting a User Group](#)" on page 153.

To delete a device group

1. Click  [Devices](#).
2. On the left side of the resulting page, move the mouse over the name of the device group that you want to delete.

An icon is now shown to the right of the name.

3. Click the  icon.

Managing a Device

When you click the entry for a device on the **All Devices** page to display the device information, several tabs are shown. The number of tabs depends on whether the mobile device management has been allowed or not. The mobile device management can only be allowed from the app store client on the mobile device.

The following tabs are always shown:

Tab	Description
Device	<p>This tab shows information on the device such as the model or operating system and the commands that can be used to manage the device.</p> <p>If the mobile device management has not been allowed on the device, only one button is shown on this page:</p> <ul style="list-style-type: none"> ■ Remove Device. See "Removing a Device" on page 120. <p>If the mobile device management has been allowed on the device, the following buttons are shown:</p> <ul style="list-style-type: none"> ■ Lock Device Now. See "Remotely Locking a Device" on page 117. ■ Update Device Info. See "Updating the Device Information" on page 117. ■ Wipe Device Now. See "Remotely Wiping a Device" on page 118. ■ Ping Device. See "Pinging a Device" on page 118. ■ Remove MDM. See "Removing the Mobile Device Management (MDM) from a Device" on page 119.
Applications	<p>This tab lists the apps from your app store that are installed on this device, and indicates for each app whether this is the latest version. If the mobile device management has been allowed on the device, the Remove Selected Apps button is shown. A check box is then shown for each app that can be removed from the device.</p> <p>You can click an app to display information about it (see also "Displaying an App" on page 61). If the mobile device management has been allowed on the device, you can also update or force the removal of an obsolete app from the Devices page of the app (see "Managing the Devices on Which the App Can be Installed" on page 100).</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: If the apps installed on your mobile device are not shown in Mobile Administrator, go to the Device tab and click Update Device Info. Keep in mind that this is only possible when the mobile device management has been allowed on the device.</p> </div> <p>Sometimes, an app which has already been uninstalled on the mobile device is still listed in Mobile Administrator. Mobile</p>

Tab	Description
	Administrator will only notice the uninstallation (on iOS) when the app store client is restarted after the uninstallation.

The following additional tabs are shown if the mobile device management has been allowed on the device:

Tab	Description
Policies	This tab lists the policies that are currently applied to this device. You can add and remove policies.
Commands	This tab shows the history of interactions with the device. See "Viewing the Commands that have been Sent to a Device" on page 118.


Note: If you want to view the devices onto which a specific app has been downloaded, see the **Devices** page of the app. In this case, you can also install, update or remove the app. See ["Managing the Devices on Which the App Can be Installed"](#) on page 100.

Adding Policies to a Device

You can add policies to a single device if the mobile device management has been allowed on that device. In this case, a **Policies** tab is shown when you display the device.

The policies can be added to the devices in addition to any defined group policies.


To add policies to a device

1. Click  **Devices**.
2. Click the entry for the device to which you want to add a policy.
3. Click the **Policies** tab.
4. Select the policy from the drop-down list box and click **Add Policy**.

Removing Policies from a Device

If the mobile device management has been allowed on a device, you can remove any policies which have been added directly to this device. It is not possible, however, to remove group policies from a device. They can only be removed by removing the device from the group.

To remove policies from a device

1. Click  **Devices**.
2. Click the entry for the device from which you want to remove a policy.
3. Click the **Policies** tab.
4. Select the check box for each policy that you want to remove and click **Remove Selected Policies**.

A dialog box appears, asking whether you are sure.


5. Click **OK** to confirm the removal.

Remotely Locking a Device

If the mobile device management has been allowed on a device, you can lock this device. The effect is the same as switching off the display by pressing the device's power button. This is useful when the device has been lost.

Caution: Locking a lost device is only useful if a passcode has been set on the device. If a device can be used without entering a passcode, the following message is shown next to the **Lock Device Now** button: "No passcode set on this device". In this case, locking does not make sense and you should consider to wipe the device.

To lock a device


1. Click  **Devices**.
2. Click the link for the device that you want to lock.
3. On the **Device** tab, click **Lock Device Now**.

The device is locked immediately. You are not prompted to confirm this command.

Updating the Device Information

If the mobile device management has been allowed on a device, you can request an update of general device information, such as the device's name and installed apps.

To update the device information


1. Click  **Devices**.
2. Click the link for the device for which you want to update the information.
3. On the **Device** tab, click **Update Device Info**.

Note: To view the updated device info, go to the **Commands** tab and check the latest `UpdateInfoCommand` entry. See "[Viewing the Commands that have been Sent to a Device](#)" on page 118.

Remotely Wiping a Device

If the mobile device management has been allowed on a device, you can erase (wipe) all data on this device. This is helpful if the device has been lost or stolen. No warning is given to the user. The command is performed immediately even if the device is locked.


To wipe a device

1. Click  **Devices**.
2. Click the link for the device that you want to wipe.
3. On the **Device** tab, click **Wipe Device Now**.
A dialog box appears, asking whether you are sure.
4. Click **OK** to confirm that all data will be erased.

Pinging a Device

If the mobile device management has been allowed on a device, you can ping this device. This is helpful if you want to check whether a device is responding to Mobile Administrator. A push notification will then be sent to the device, asking the device to respond.

To ping a device

1. Click  **Devices**.
2. Click the link for the device that you want to ping.
3. On the **Device** tab, click **Ping Device**.

The response from the device is shown next to the button. You should see a response such as "This device was last seen less than a minute ago".

If the previously shown response (for example, "This device was last seen 7 days ago") does not change, this may mean that the device is currently switched off or that it is currently not able to send and receive mobile data.

Viewing the Commands that have been Sent to a Device

You can view the commands that have been sent to a single device if the mobile device management has been allowed on that device. In this case, a **Commands** tab is shown when you display the device.

Examples of such commands are:


- `InstallAppCommand`. See ["Installing an App on a Managed Device"](#) on page 101.
- `RemoveAppCommand`. See ["Removing an App from a Managed Device"](#) on page 101.
- `ApplyPoliciesCommand`. See ["Adding Policies to a Device"](#) on page 116.
- `LockDeviceCommand`. See ["Remotely Locking a Device"](#) on page 117.
- `UpdateInfoCommand`. See ["Updating the Device Information"](#) on page 117.

The status of a command can be one of the following:

- **Created**. Shown when the command has not yet been sent, or when an answer has not yet been received.
- **Success**. Shown when the command has successfully been processed on the device, for example, when an app has been installed, or when policies have been applied.
- **Error**. Shown when the command could not be processed on the device, for example, when the user has rejected the installation of an app.
- **Invalid**. Shown when the execution of a newly created command has been prevented as described below.

You can click a command to display detailed processing information. When a command is still in the status "Created", an **Invalidate** button is provided. You can click this button if you want to prevent the execution of the command.

To view the commands that have been sent to a device

1. Click  **Devices**.
2. Click the link for the device that you want to view.
3. Click the **Commands** tab.

All commands that have been sent to the device are now shown.

4. To view detailed processing information for a command, click the entry for that command.


Removing the Mobile Device Management (MDM) from a Device

If the mobile device management has been allowed on a device, you can remotely remove the mobile device management. This would be done, for example, when an employee leaves the company for whom a "bring your own device" (BYOD) policy is currently in place.

When you remove the device management association from a device, this will remove any of your organization-specific policies, certificates, email accounts and apps while leaving the rest of the device as-is. You will not be able to send any more commands to the device after the mobile device management has been removed.

This command is only shown for an administrator. The end user can disable the mobile device management directly on the mobile device.

To remove the mobile device management from a device

1. Click  **Devices**.
2. Click the link for the device from which you want to remove the mobile device management.
3. On the **Device** tab, click **Remove MDM**.
A dialog box appears, asking whether you are sure.
4. Click **OK** to confirm the removal.


Removing a Device

You can only remove a device, if the mobile device management has not been allowed on the device.

When you remove a device, it is removed from the **All Devices** page. However, the next time this device is used to access your app store client, it will be shown again on that page.

Removing a device is helpful, for example, after having debugged an app with the help of that device, or if Mobile Administrator still lists company-owned devices that are no longer used.

To remove a device

1. Click  **Devices**.
2. Click the link for the device that you want to remove.
3. On the **Device** tab, click **Remove Device**.
A dialog box appears, asking whether you are sure.
4. Click **OK** to confirm the removal.

5 Managing Policies

■ Overview	122
■ The All Policies Page	122
■ Adding a Device Policy	123
■ Viewing the Policy Details	123
■ Editing a Device Policy	124
■ Deleting a Device Policy	124
■ Policy Types	125

Overview


Mobile Administrator distinguishes the following types of policies:

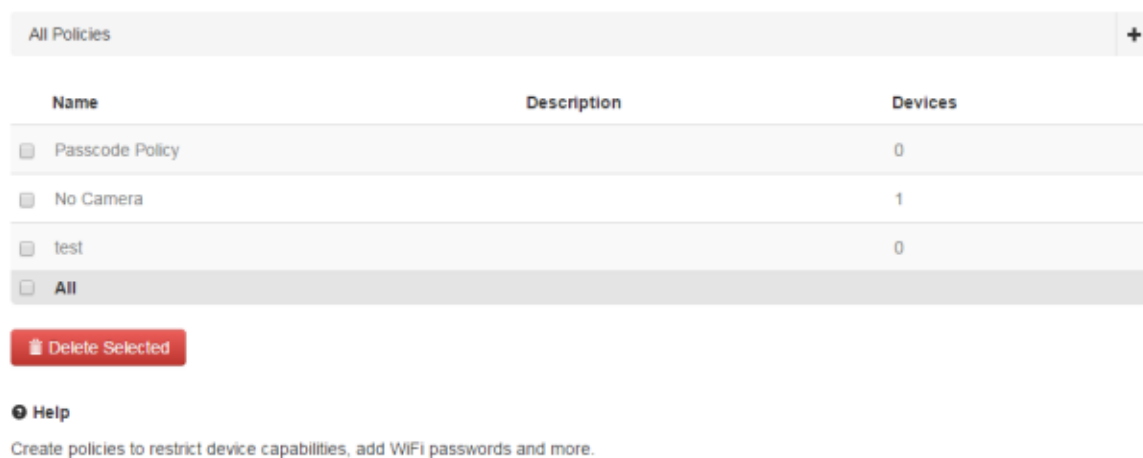
- **Device Policies.** The device policies are used to restrict device capabilities, add WiFi passwords and more. They can be applied to all devices in a specific group or, if the mobile device management has been allowed on the devices, to single devices. See also ["Policy Types" on page 125](#).
- **App Policies.** Instead of relying only on devices fully managed by the enterprise, it is also possible to enforce app policies. This enables the same mobile device for both private and business usage without compromising confidential data of your enterprise. App policies can, for example, deactivate copying text within your apps, even if the device is not managed by your IT department. The app policies can be defined when adding or editing a build configuration for an app. See also ["Overview of App Policies" on page 88](#).

This chapter provides information on the device policies. To create and remove device policies, you need the site-level permissions **Manage Policies**. See also ["Overview of Site-Level Permissions" on page 141](#).

Note: The device policies only apply for iOS and Android. They do not apply to Windows Phone as the mobile device management for this platform is not supported.

The All Policies Page

When you click  **Policies**, the **All Policies** page is shown which lists all device policies which are currently defined, together with the number of devices on which a policy is active.



Name	Description	Devices
<input type="checkbox"/> Passcode Policy		0
<input type="checkbox"/> No Camera		1
<input type="checkbox"/> test		0
<input type="checkbox"/> All		0

Delete Selected


Help
Create policies to restrict device capabilities, add WiFi passwords and more.

Using this page, you can add new device policies, display and edit existing device policies, or delete existing device policies.

Adding a Device Policy

Mobile Administrator comes with a number of predefined policy types. When you add a device policy, you select a policy type, give it a name and specify all required options. For example, you can add a policy of type "Restrictions", give it the name "Disable camera" and then enable only the "Restrict use of camera" option. When you go to the **All Devices** page, you can then add the new "Disable Camera" policy to a device group or user group. Or you can display a single managed device, go to the **Policies** tab (which is only shown for managed devices), and then add the new "Disable camera" policy to that device.

To add a device policy

1. Click  **Policies**.
2. On the **All Policies** page, click .
3. On the resulting page, specify the following information:

Option	Description
Policy type	Select the policy type from the drop-down list box.
Name	Type the name of the policy.
Description	Optional. Type a brief description of the policy.

The remaining options on this page depend on the policy type that you have selected.


4. Specify all required options for the selected policy type. See "[Policy Types](#)" on page 125.
5. Click **Create Policy**.

The **Policy Details** page appears, providing information on the policy you have just added.

Viewing the Policy Details

The policy details tell you when a device policy has been created and last modified, and they show at a glance the policy options which have been specified.


To view the policy details

1. Click  [Policies](#).
2. On the **All Policies** page, click the policy that you want to view.

Editing a Device Policy

You can change the policy name, the description and all policy options. The changed policy will automatically be applied to all devices which use this policy.


To edit a device policy

1. Click  [Policies](#).
2. On the **All Policies** page, click the link for the policy that you want to edit.
3. Click **Edit Policy**.
4. Change all required options for the selected policy type. See "[Policy Types](#)" on page 125.
5. Click **Update Policy**.

Deleting a Device Policy

When you delete a device policy, it is removed from all device groups, user groups and single devices to which this policy has been applied. It is consequently also removed from all devices on which this policy is currently active.

To delete a device policy

1. Click  [Policies](#).
2. On the **All Policies** page, do one of the following:
 - Select the check box for each policy that you want to delete and click **Delete Selected**.
 - Or click the link for a policy to display the policy details and then click **Delete Policy**.

A dialog box appears, asking whether you are sure.

3. Click **OK** to confirm the deletion.

Policy Types

Exchange Account Policy

Availability: iOS 5.0 and above.

Allows the configuration of a Microsoft Exchange account on the mobile device for mail, contacts and calendar access.

<u>Option</u>	<u>Description</u>
Host name	Enter the name of the Exchange server.
SSL enabled	Select this option if SSL has been enabled on the Exchange server.
Domain	Enter the domain in which the Exchange server is located.
Username	Either leave the text box blank to use the user name of the device owner, or enter the user name as defined for the Exchange account.
Password	Either leave the text box blank if the user has to enter the password for the Exchange account on the device, or enter a password.
Prevent move	If selected, the user is not able to move messages from the account.

Home Button Policy

Availability: iOS 5.0 and above.

Limits the usage of the mobile device to a single app by disabling the home button completely. The device needs to be restarted after the policy has been applied, and the first app that is launched becomes the "locked" app.

<u>Option</u>	<u>Description</u>
Disable home button	If selected, the user cannot use the home button of the mobile device.

Passcode Policy

Availability: iOS 5.0 and above, Android 2.3 and above.

Defines detailed rules forcing a PIN or passcode to be set on the mobile device.

Option	Description
Require passcode	<p>If selected, the user is forced to set a passcode on the mobile device. All other passcode options (see below) will then be taken into account.</p> <p>If not selected, the user is not forced to set a passcode. In this case, the user is free to decide whether to set a passcode or not. The settings of the options below will not have any effect.</p>
Minimum length	Enter the minimum length of the passcode.
Require alphanumeric passcode	If selected, the user has to set a passcode that consists of letters, numbers and special characters.
Password expiration timeout	Enter the number of days after which the password expires. If you leave the text box blank, the password will not expire.
Password history restriction	Enter the number of new unique passwords that the user has to enter before the user can reuse a previous password. If you leave the text box blank, this restriction will not be enabled.
Maximum failed password attempts	Select the number of failed password attempts (2 though 10 attempts) after which the device is locked or wiped, depending on the platform.
Maximum inactivity time lock	Select the number of minutes after which the lock screen of the device will be activated.

Restrictions Policy

Availability: iOS 5.0 and above, Android 4.0 and above.

Restricts general device capabilities such as disabling the built-in camera or the ability to take screenshots.

Note: These options mainly pertain to iOS. Android only supports the **Restrict use of camera** option.

Option	Description
Restrict installing apps	If selected, the user cannot install any apps on the mobile device.
Restrict use of camera	If selected, the mobile device cannot be used to take photos.
Restrict screen capture	If selected, the mobile device cannot be used to make screenshots.
Restrict Siri	If selected, the voice recognition system Siri cannot be used on the mobile device.
Restrict use of YouTube	If selected, YouTube cannot be used on the mobile device.
Restrict use of iTunes	If selected, iTunes cannot be used on the mobile device.
Restrict In-App Purchases	If selected, in-app purchases are disabled on the mobile device.
Restrict use of Safari	If selected, the Safari browser cannot be used on the mobile device. Other browsers can still be used. It is recommended that you use this policy together with the Restrict installing apps policy.
Restrict iCloud backup	If selected, the mobile device cannot use the iCloud for backups.
Restrict iCloud document sync	If selected, the mobile device cannot use the iCloud to synchronize documents.
Restrict Photo Stream	If selected, the mobile device cannot use the Photo Stream to upload photos to the iCloud.

Caution: Disallowing this can cause data loss.

Option	Description
Force encrypted backups	If selected, backups to iTunes will be encrypted. This will require a password if the backup is to be restored.
Restrict multiplayer gaming	If selected, the mobile device cannot be used for multiplayer games within the Game Center.
Restrict adding Game Center friends	If selected, the mobile device cannot be used to add friends to the Game Center.

VPN Service Policy

Availability: iOS 5.0 and above.

Allows the configuration of a VPN (virtual private network) account on the mobile device.

Option	Description
Send all traffic through the VPN interface	<p>If not selected (default), VPN is only used for certain requests. For example, when an internal server can only be reached via VPN, VPN will be used. For all other data which can be sent via a browser or an app where VPN is not required, VPN will not be used.</p> <p>If selected, all traffic is sent through the VPN interface.</p>
VPN type	Select the VPN type. Supported VPN types are IPSec, PPTP and L2TP.
VPN connection should be brought up on demand	<p>If not selected (default), VPN is always active.</p> <p>If selected, the VPN connection is only established when needed.</p>
IP address or host name of the VPN server	Type the IP address of host name of the VPN server.
User name for VPN account	Either leave the text box blank to use the user name of the device owner, or enter the user name as defined for the VPN account.

Option	Description
Xauth enabled	If selected, the users are authenticated against Xauth.
Group name	Type the name of the VPN group.
Shared secret	Type the shared secret for establishing a secure connection.
Prompt for a PIN when connecting	If selected, the user has to enter a PIN when connecting to the VPN.

Web Clip Policy

Availability: iOS 5.0 and above.

Adds a web clip icon (bookmark) with a specified URL to the user's home screen.

Option	Description
Label	Type the name that is to be shown for the web clip icon.
URL	Type the URL for the website that is to be accessed.
Removable	If selected, the user is able to remove the web clip icon from the home screen.
Full screen	If selected, the website that is accessed via the web clip icon is shown in full-screen mode.

WiFi Network Policy

Availability: iOS 5.0 and above, Android 4.0 and above.


Allows the configuration of a WiFi network (pre-shared key) on the mobile device.

Option	Description
WiFi name	Type the name of the WiFi network.
WiFi password	Type the password that is used for accessing the WiFi network.

6 Managing Domains


■ Overview	132
■ The All Domains Page	132
■ Viewing the Domain Details	132
■ Editing the Domain	133
■ Allowing Access for Users from an LDAP Directory	135
■ Creating a New Domain	136
■ Checking the Space Usage	137
■ Viewing the MDM Certificates	137
■ Deleting a Domain	138

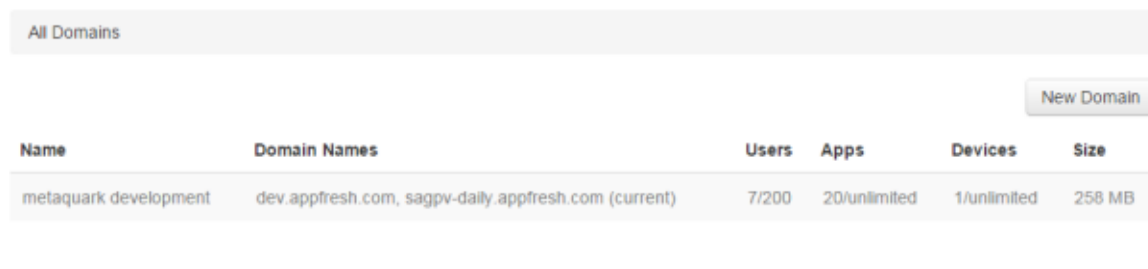
Overview

One Mobile Administrator instance can host multiple domains. Depending on your permissions, the  menu contains one of the following commands:

- **Domains.** This command is shown if you have the site-level permission **Manage All Sites**. When you click **Domains**, a list of all defined domains is shown and you can click a domain to display its details. With this permission, you are also allowed to create and delete domains.
- **Domain.** This command is shown if you only have the site-level permission **Manage Site**. When you click **Domain**, the details for the domain to which you are currently logged in are immediately shown.

The All Domains Page

When you click  and then **Domains**, the **All Domains** page is shown which lists all domains which are currently defined. For each domain, the number of users, apps and managed devices is shown, followed by the limits of your license file. You can also see how much disk space is used by each domain. Keep in mind that you can only display this page if you have the site-level permission **Manage All Sites**.



Name	Domain Names	Users	Apps	Devices	Size
metaquark development	dev.appfresh.com, sagpv-daily.appfresh.com (current)	7/200	20/unlimited	1/unlimited	258 MB

Using this page, you can add new domains and configure existing domains.

Each domain that you add is initially empty and you have to configure it. The configuration of another domain can be done in the domain in which you are currently logged in. If you want to add apps to another domain and define the users that are allowed to use this domain, however, you have to log out from the current domain and log in to the other domain using the appropriate URL.



Viewing the Domain Details

The **Domain Details** page shows you at a glance the information that has been defined for a domain. This also includes information as to the validity of your license file. You use this page to configure the domain. Different buttons are provided that allow you to edit the domain and thus also define the LDAP users who are allowed to access this

domain, to view the space usage of your apps, and to manage the MDM certificates for iOS.

Note: Directly after the installation, you can comfortably configure Mobile Administrator using the Configuration Assistant which can be invoked from this page. See also "[Configuring Mobile Administrator](#)" on page 27.



To view the domain details

- If you have the site-level permission **Manage All Sites**, do the following:
 1. Click  and then **Domains**.
 2. On the **All Domains** page, click the entry for the domain.
- If you only have the site-level permission **Manage Site**, click  and then **Domain**.


Editing the Domain

Most details can be changed if you have the site-level permission **Manage Site**. Some details, however, such as the domain name and the CA information can only be changed if you have the site-level permission **Manage All Sites**.

To edit the domain

1. Do one of the following, depending on your permissions:
 - Click  and then **Domains**. On the resulting page, click the entry for the domain.
 - Or click  and then **Domain**.
2. Click **Edit Domain**.
3. Specify all required information:

Option	Description
Company name	Enter a company name. This name will be used in the emails that are sent by Mobile Administrator.
Domain names	You have to specify at least one domain name (for example, <code>my.domain.com</code>). If you want to define alternative domain names, you have to separate them using a comma. Make sure that the domain names that you specify are configured on the server. If required, ask your system administrator to register the new domain.

<u>Option</u>	<u>Description</u>
License	Click Browse and then select the license file that you have received from Software AG. See also " Adding the Mobile Administrator License File " on page 30.
Email from	The name and address to be used as the sender information when Mobile Administrator sends mail (for example, when a user want to reset the password).
Admin email	The real mail address of the administrator. All mail to the administrator will be sent to this address. If you set both, Email from and Admin email , a mail will be sent to the Admin email address, but the name and address defined in Email from will be used as the sender information.
Logo	Click Browse and then select the file containing the image that is to be shown on the login page and on the home button in the navigation bar. You can upload a PNG, JPG or GIF file.
Terms of Service	Enter or paste the text that is to be shown in a dialog in the app store client or in the browser. When you set or update your Terms of Service here, every user will be prompted to accept them upon the next visit, that is, when logging in to Mobile Administrator in the browser (PC and mobile device) or when invoking your client app store on the mobile device. Tip: If you need more space for your text, move the mouse pointer to the bottom right corner of the text box (). The mouse pointer changes and you can now resize the text box.
Intermediate CA	Click Browse and then select the intermediate CA certificate file (PEM/P12).
Intermediate CA Password	Enter the password for the intermediate CA certificate.
Trust CA	Optional. Click Browse and then select the trust CA certificate file (PEM/CER).
GCM API Key	You have to specify a Google Cloud Messaging (GCM) API key if you want to support mobile device

Option	Description
	management (MDM) and push notifications on Android devices. For more information on how to obtain such a key, see http://developer.android.com/google/gcm/gs.html .
Windows Phone 8 application enrollment token	You have to upload such a token if you want to make available your apps on Windows Phone devices. You receive the token when you register for the Windows Phone Dev Center. Click Browse and then select the AETX file.

Note: For information on the LDAP configuration, see "[Allowing Access for Users from an LDAP Directory](#)" on page 135.



4. Click **Update Site**.

Allowing Access for Users from an LDAP Directory

When you edit a domain, you can optionally specify information for connecting to an LDAP server. The configured LDAP users will then be able to log in to Mobile Administrator and the app store. For more information, see "[Managing Users](#)" on page 139.

As a rule, a company only uses a single LDAP server. If you need to define an additional LDAP server, you have to create an additional domain. See "[Creating a New Domain](#)" on page 136.

To allow access for users from an LDAP directory

1. Do one of the following, depending on your permissions:
 - Click  and then **Domains**. On the resulting page, click the entry for the domain.
 - Or click  and then **Domain**.
2. Click **Edit Domain**.
3. Scroll down to the section **LDAP Configuration**.
4. Specify the following information for the LDAP server:

Option	Description
Host name	The name of the LDAP server (for example, <code>ldap.acme.corp</code>).

Option	Description
Port	Optional. The port on which the LDAP server is running. If omitted, the default port 389 is used for standard connections (<code>ldap</code>) or 636 is used for secure connections (<code>ldaps</code>).
base	The base DN (that is, the top level) of your LDAP directory tree (for example, <code>dc=domain, dc=com</code>).
Password	The password for connecting to the LDAP server.
bind_dn	The user with whom the connection to the LDAP is to be established (for example, <code>cn=administrator</code>).

- To define the user and group schemes, specify the following information under the corresponding headings:

Option	Description
dn	The distinguished name for the user or group schema.
prefix	A prefix such as the common name (for example <code>cn=users</code> or <code>cn=groups</code>).
classes	An object class (for example, <code>person</code> or <code>PosixGroup</code>).

Note: For more detailed information on the string representation of distinguished names, see <http://www.ietf.org/rfc/rfc4514.txt?number=2253>.

- Click **Update Site**.


Creating a New Domain

In addition to the default domain that comes with Mobile Administrator, you can create additional domains which run on the same hardware. For example, you may want to create a new domain if you want to make available apps that you do not want to offer in the current domain to a different group of users. To do so, you need the site-level permission **Manage All Sites**.

To build the app store client for the new domain, to define the apps for the new domain and to define the users that are allowed to use this domain, you have to log out from the

current domain and log in to the new domain using the appropriate URL. You can then configure the new domain as described in ["Configuring Mobile Administrator" on page 27](#).

To create a new domain


1. Click  and then **Domains**.
2. On the **All Domains** page, click **New Domain**.
3. Specify all required information. The options are the same as when editing a domain. See ["Editing the Domain" on page 133](#).
4. Optional. Define the LDAP configuration. See ["Allowing Access for Users from an LDAP Directory" on page 135](#) for detailed information on the options that you can specify.
5. Click **Create Site**.

Checking the Space Usage

If you have the site-level permission **Manage All Sites**, you can check how much disk space is used by each app (that is, by the app versions, the build jobs and the resources of the apps).

When you display the space usage for a new domain that has just been added, you will see an entry for the app store client. As long as you have not built the app store client as described in ["Creating and Launching Build Configurations for the App Store Client" on page 41](#), the space usage will be 0 bytes.

To check the space usage

1. Click  and then **Domains**.
2. On the **All Domains** page, click the entry for the domain that you want to check
3. Click **Space Usage**.



The resulting page shows all apps. For each app, you can see how much space is used for the app versions, the build jobs, and resources. If you want to free up space, click an app name and then delete anything that is no longer needed.

Viewing the MDM Certificates

An MDM certificate is required if you want to support the mobile device management (MDM) on iOS devices.

To view the available MDM certificates

1. Do one of the following, depending on your permissions:


- Click  and then **Domains**. On the resulting page, click the entry for the domain.
 - Or click  and then **Domain**.
2. Scroll down to the heading **MDM Certificates**.
If certificates have already been defined, they are shown under this heading. The state ("active" or "expired") and the expiration date are shown for each certificate.
 3. To upload a new certificate, click **New Certificate**. For more information, see ["Uploading an MDM Certificate for iOS" on page 45](#).

Deleting a Domain

You can delete a domain if you have the site-level permission **Manage All Sites**.

Caution: If you delete all domains, including the default domain, Mobile Administrator can no longer be used. You have to reinstall Mobile Administrator and configure the domain once more.

To delete a domain

1. Click  and then **Domains**.
2. On the **All Domains** page, click the entry for the domain that you want to delete.
3. Click **Delete Domain**.
A dialog appears, asking whether you are really sure.
4. Click **OK** to confirm the deletion.

7 Managing Users


■ Overview	140
■ The All Users Page	140
■ Overview of Site-Level Permissions	141
■ Adding a Local User	142
■ Managing the User Details	143
■ Adding a User to a Local User Group	148
■ Removing a User from a Local User Group	148
■ Deleting a User	149

Overview


Users can be added manually with Mobile Administrator, but more usually they will be authenticated against an LDAP server (see also ["Allowing Access for Users from an LDAP Directory" on page 135](#)). Mobile Administrator distinguishes the following types of users:

- **Local users.** You can manually add local users to allow individual users to access Mobile Administrator and the app store. You can grant separate application-level and site-level permissions for each user.
- **LDAP users.** LDAP users are added automatically to Mobile Administrator. When you have connected to an LDAP server, a local reference to an LDAP user entry is automatically created on the **All Users** page when the user first logs in to Mobile Administrator. References are also created for any LDAP groups in which the user is a member. The LDAP group memberships are updated every time an LDAP users logs in. The name, password and email address of an LDAP user cannot be changed with Mobile Administrator. This can only be changed directly in the LDAP directory. However, you can use Mobile Administrator to grant application-level and site-level permissions for the LDAP users.

To add local users and to manage local and LDAP users, you need the site-level permission **Manage Users and Groups**.

Note: If you are a normal user without any administrator rights, you can only change your own user profile via the  ▾ menu. See also ["Checking the User Profile" on page 17](#).

The All Users Page

When you click  ▾ and then **Users**, the **All Users** page is shown which lists all currently defined users, along with the date on which the user has last accessed Mobile Administrator and the number of groups to which a user belongs. Each user always belongs to at least one group, the "All Users" group. The type "Local" is shown for a user who has been added manually. The type "LDAP" is shown for an LDAP user entry that has been created automatically when the user has logged in to Mobile Administrator for the first time.

All Users

Filter: + ▾

Username	First name	Last name	Type	Last Seen	Groups
admin			Local	2014-08-22	1
buildnode			Local	2014-08-22	1
tAdministrator			Local	2013-12-09	2
tDeveloper			Local	2014-08-22	2

Add to Group ▾
 Remove from Group ▾
 Delete

Tip: You can also access this page from the dashboard: In the **Domain Information** box, click the number that is shown next to **Active Users**.

Using this page, you can add local users to Mobile Administrator, add users to a user group, remove users from a user group, delete users, or display and edit the user details.

Using the **Filter** box, you can restrict the list to show only those users that meet your filter criteria. For example, you can only display the users who have last been seen on a specific day or in a specific month. See also "[Filtering Lists](#)" on page 22.

Overview of Site-Level Permissions

The site-level permissions are granted to users. They can be granted to both, users that have manually been added and users from an LDAP.

To grant site-level permissions to other users, you need the site-level permission **Manage Admin Permissions**.

The following site-level permissions exist:

Permission	Description
Add Apps	May add new applications (the creating user is granted all app specific rights for the newly created app).
Manage Apps	May manage applications; this includes all app specific permissions for all apps.
Manage Policies	May create and remove device policies.
Assign Policies	May assign existing device policies to devices.

Permission	Description
Manage Devices	May organize and remove managed devices.
Wipe Devices	May remotely wipe managed devices.
Manage Users and Groups	May manage local users and user groups on this site.
Manage Admin Permissions	May assign site admin permissions to users (from this list of permissions).
Manage Site	May edit site information, such as domain names, certificates and licenses.
Manage All Sites	May manage all sites on this instance.



Note: You can also grant application-level permissions to a user. To do so, you must go to the app and modify the permissions there. See "[Overview of Application-Level Permissions](#)" on page 84.

Adding a Local User

If you do not use an LDAP server, you have to add all users manually to whom you want to grant access to Mobile Administrator and the app store. These are the so-called local users.

If you are using an LDAP server and you have already configured the LDAP access in Mobile Administrator, you can also add local users, in addition to the LDAP users.

To add a local user

1. Click  and then **Users**.
2. On the **All Users** page, click .
3. On the resulting page, specify the following information:

Option	Description
Username	The name that is to be used to log in to Mobile Administrator or your app store.
First name	Optional. The first name of the user.

Option	Description
Last name	Optional. The last name of the user.
New password	The password for the user.
Confirm new password	Optional. Enter the password once more to confirm it.
Active	<p>If selected (default), the user is able to log in to Mobile Administrator or your app store.</p> <p>If not selected, the user is not able to log in to Mobile Administrator or your app store. This is helpful, for example, if you prepare the accounts for new users and you want to postpone the activation to a later point in time.</p>
Email	The email address of the user.


- If you want to grant site-level (administration) permissions for the new user, select the corresponding check boxes. These permissions can only be changed by a user who has been granted the **Manage All Sites** permission. Other users do not see these options. See also "[Overview of Site-Level Permissions](#)" on page 141.
- Click **Create User**.
The new user is now shown on the **All Users** page. If it is currently not shown, check the current filter definition or the number of entries that are to be shown.
- If you want to define an avatar, notification settings or access tokens for the new user, go to the details page of the new user. See "[Managing the User Details](#)" on page 143.
- If you want to grant application-level permissions (including the right to download an app) for the new user, go to the **Permissions** page of that app. See "[Managing the Permissions of an App](#)" on page 83.

Managing the User Details

The **User Details** page is shown when you click a user entry on the **All Users** page.

All Users -- teddy

User Details

[Change Avatar](#) 

Username	teddy	Type	Local User
Name	Ted Bear	Status	Active
Email	teddy@acme.com	Last Seen	never
Permissions	Add Apps Manage Apps	Created at	2014-11-19 14:02 CET
		Updated at	2014-11-19 14:02 CET

[Edit User](#)
[Notifications](#)
[Delete User](#)

Groups

Name

All Users

Apps

There are no apps assigned to this user.

Access Tokens

There are no access tokens for this user.

[+ New Token](#)

Note: When a user displays the user profile, similar information is shown. The information that is then shown depends on the permissions which have been assigned to the user. See also "[Checking the User Profile](#)" on page 17.

When permissions have been granted to the user, they are listed on this page. If defined, you can also see the user groups to which the user belongs, the apps that have been assigned to the user (that is, the apps that the user has added), and the access tokens that the user can use.


You can change the avatar for a user, edit the user details (keep in mind that the name, password and email address of an LDAP user cannot be changed with Mobile Administrator), and specify the notifications that the user is to receive for the different apps. You can also use this page to delete the user, or to add and delete access tokens.

Changing the Avatar for a User

By default, the same grey avatar is shown for all users. For each user (local user and LDAP user), you can upload an image that is to be shown in the list of users and in the user details.

Note: If the user's email address is registered at gravator.com, this service will be used to show the "Globally Recognized Avatar", unless an image is uploaded with Mobile Administrator.

To change the avatar for a user

1. Click  and then **Users**.
2. On the **All Users** page, click the user entry to display the **User Details** page.
3. Do one of the following:
 - Click **Change Avatar** and select the image that you want to use as your avatar from the resulting dialog box.
 - Drag the image from your file system onto the **User Details** page.

Editing the User Details


For a local user, you can change the same information as when adding the user: user name, first and last name, email address, and password. You can also define whether a local user is active or not. Only an active user can log on to Mobile Administrator or your app store. Defining a user as inactive (disabled) is helpful, for example, if an employee has left the company and you do not want to delete this user immediately.

For an LDAP user, the above-mentioned information cannot be changed with Mobile Administrator. It can only be changed in the LDAP directory.

If you have the appropriate permissions, you can change the site-level permissions for a user. These permissions can be changed for both types of users: local users and LDAP users.

If you are editing your own user profile, you will not be able to define yourself as inactive. A corresponding message will appear in this case.

To edit the user details

1. Click  and then **Users**.
2. On the **All Users** page, click the user entry.
3. Click **Edit User**.
4. Local user only: Modify the user information such as the last name or email address.
5. To change the site-level permissions for the user, select or deselect the corresponding check boxes. See also "[Overview of Site-Level Permissions](#)" on page 141.

The site-level permissions can only be changed by a user who has been granted the **Manage All Sites** permission. Other users cannot see these options.

Caution: Take care when removing permissions from your own profile. For example, when you remove the **Manage Users and Groups** permission, you

will no longer be able to reenable this permission for yourself. You will then have to ask an administrator to do this.

6. Click **Update User**.

Specifying the Notifications that a User Receives

You can specify whether a user is to receive notifications for an app. A notification will be sent as an email to the email address that is defined in the user details.


There are different types of notifications:

- **Update Notifications.** The user receives an email when the app gets a new update.
- **New Comment Notifications.** The user receives an email when someone comments on an app (this includes comments in the app store).

The site-level permissions of a user determine the apps for which notifications can be sent:

- A normal user with no site-level permissions can receive notifications for the apps that are assigned to this user (that is, for the apps that the user has added).
- A user with the site-level permission **Manage Apps** can receive notifications for all currently defined apps.

To specify the notifications that a user receives

1. Click  and then **Users**.
2. On the **All Users** page, click the user entry.
3. Click **Notifications**.
4. On the resulting page, select the check box for the type of notification that the user is to receive for a specific app.

You can also select **toggle all**, which is shown at the bottom of the page, to select or deselect all check boxes in a column.

5. Click **Save**.

Adding an Access Token for a User


An access token is required when you copy an app from an other Mobile Administrator instance. See also "[Adding an App from Another Mobile Administrator Instance](#)" on [page 57](#).

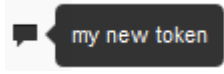
When accessing Mobile Administrator through the REST API, a user can authenticate with the user name and password. If you require more control or do not want to give out the password (for example, when running a build node), API access can be granted by creating an access token for the user. Any API access that is authenticated using an access token has the same permissions as the user to whom the access token is attached.

For more information, see the following guide: *webMethods Mobile Administrator API Reference*.

Access tokens can be limited to be valid only until a specific date or for a limited number of uses. They can be removed at any time.

To add an access token for a user

1. Click  and then **Users**.
2. On the **All Users** page, click the user entry.
3. Click **New Token** (located at the bottom of the page).
4. Optional. Specify the following information:


Option	Description
Valid Until	<p>By default, there is no restriction as to the time range in which an access token is valid.</p> <p>If you want to restrict the validity, clear the Unlimited check box and then define the date and time until when this access token is valid.</p>
Remaining Uses	<p>By default, there is no restriction as to how often an access token can be used.</p> <p>If you want to restrict the usage, clear the Unlimited check box and then define the number of remaining uses. The number of remaining uses will then be decreased each time the access token is used.</p>
Comment	<p>Type a brief comment. This comment can be viewed as a tooltip from the User Details page by moving the mouse over the icon that is shown at the very right of the token entry. For example:</p>  <p>The comment cannot be changed once the token has been created.</p>

5. Click **Add Token**.

Deleting an Access Token for a User

You can delete an access token if the user should no longer be able to use it or when the access token is no longer valid.

To delete an access token for a user


1. Click  and then **Users**.
2. On the **All Users** page, click the user entry.
3. Scroll down to the list of access tokens and select the check box for the access token that you want to delete.
4. Click **Delete**.
You are asked whether you are sure.
5. Click **OK** to confirm the deletion.

Adding a User to a Local User Group

You can add local users and LDAP users to existing local user groups. A user may belong to one or more groups.

Note: For information on how to create local user groups, see "[Creating a Local User Group](#)" on page 152.

To add a user to a local user group


1. Click  and then **Users**.
2. On the **All Users** page, do one of the following:
 - Click the check box for each user that you want to add to a local user group.
 - Or click the check box at the bottom to select all users.
3. Click **Add to Group**.
4. In the resulting drop-down list, click the name of the local user group to which you want to add the selected users.

Removing a User from a Local User Group

If users have been added to a local user group, they can be removed from that group.

Note: It is not possible to remove a user from the **All Users** group.

To remove a user from a local user group

1. Click  and then **Users**.
2. On the **All Users** page, do one of the following:

- Click the check box for each user that you want to remove from a local user group.
 - Or click the check box at the bottom to select all users.
3. Click **Remove from Group**.
 4. In the resulting drop-down list, click the name of the local user group from which you want to remove the selected users.


Deleting a User

When an employee leaves the company, you can delete the corresponding entry from the **All Users** page to disallow access to Mobile Administrator. All mobile devices that are associated with the deleted user are automatically deleted from the **All Devices** page. See also "[Managing Devices](#)" on page 109.

You can delete both local users and LDAP users. However, keep in mind that this does not automatically delete an LDAP user from the LDAP directory. When a deleted LDAP user logs in again to Mobile Administrator, the corresponding entries will reappear on the **All Users** and **All Devices** pages.

If you want to disallow the access for all LDAP users, edit the domain as described in "[Allowing Access for Users from an LDAP Directory](#)" on page 135 and delete all information that has been specified for the LDAP server. The LDAP users and their mobile devices are then automatically deleted from the **All Users** and **All Devices** pages.

To delete a user

1. Click  and then **Users**.
2. On the **All Users** page, do one of the following:
 - Select the check box for each user that you want to delete and click **Delete**.
 - Or, if you just want to delete a single user, click the user entry to display the user and then click **Delete User**.

A dialog box appears, asking whether you are sure.

3. Click **OK** to confirm the deletion.

8 Managing User Groups

■ Overview	152
■ The All User Groups Page	152
■ Creating a Local User Group	152
■ Viewing the Members of a User Group	153
■ Changing the Name of a Local User Group	153
■ Deleting a User Group	153


Overview

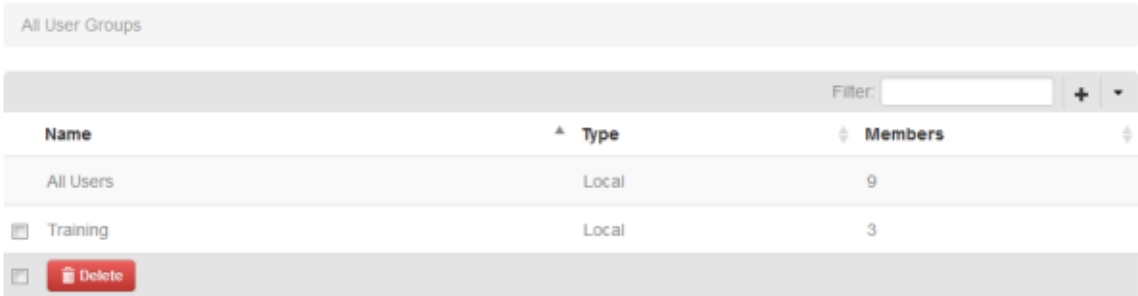
For easier permission management, you can create named user groups from the **All User Groups** page. You assign users to these groups from the **All Users** page (see ["Managing Users" on page 139](#)). Any application-level permissions can be assigned to an individual user group (see ["Overview of Application-Level Permissions" on page 84](#)). The permissions are then granted to all members of this user group.

You can assign local users and LDAP users to your user groups. For LDAP users and groups, you define the permissions just like you would for local users.

To manage the user groups on the current site, you need the site-level permission **Manage Users and Groups**. See also ["Overview of Site-Level Permissions" on page 141](#).

The All User Groups Page

When you click  and then **Groups**, the **All User Groups** page is shown which lists all currently defined user groups and the number of members in each group. The type "Local" is shown for a user group that has been created manually. The type "LDAP" is shown for an LDAP user group that has been added automatically to Mobile Administrator.



Name	Type	Members
All Users	Local	9
Training	Local	3

Using this page, you can add new user groups, delete user groups, or display the user group details.

Using the **Filter** box, you can restrict the list to show only those user groups that meet your filter criteria. See also ["Filtering Lists" on page 22](#).

Creating a Local User Group

Adding users to groups such as "Sales", "Marketing" or "External Employees" is useful when it comes to targeting the right audience for a specific app.

To create a local user group

1. Click  and then **Groups**.


2. On the **All User Groups** page, click **+**.
3. On the resulting page, specify a name for the user group.
4. Click **Create User Group**.

You can now add local users and LDAP users to the new user group. See "[Adding a User to a Local User Group](#)" on page 148.

Viewing the Members of a User Group

When you display the user group details, you can see a list of all users who are members of the group. For information on how to define the members of the user group, see "[Adding a User to a Local User Group](#)" on page 148.

To view the member assigned to a user group

1. Click  and then **Groups**.
2. On the **All User Groups** page, click the name of the user group.


The members are shown at the bottom of the resulting page. You can click a user name to display the user details.

Changing the Name of a Local User Group

If you want to change the name of a local user group, you have to edit the user group.

Note: The user group "All Users" cannot be renamed. It is also not possible to rename LDAP user groups.

To change the name of a local user group

1. Click  and then **Groups**.
2. On the **All User Groups** page, click the name of the user group.
3. Click **Edit User Group**.
4. Change the name on the resulting page.
5. Click **Update User Group**.


Deleting a User Group

When you delete a user group, you do not delete the users that are defined as members of that group. The users can still be seen when you view the user group "All Users".

You can delete both local user groups and LDAP user groups. However, keep in mind that this does not automatically delete an LDAP user group from the LDAP directory. When an LDAP user who is a member of the deleted user group logs in again to Mobile Administrator, that user group will reappear on the **All User Groups** page.

Note: The user group "All Users" cannot be deleted.

To delete a user group

1. Click  and then **Groups**.
2. On the **All User Groups** page, do one of the following:
 - Select the check box for the user group that you want to delete and click **Delete**.
 - Or click the name of the group to display it and then click **Delete User Group**.A dialog box appears, asking whether you are sure.
3. Click **OK** to confirm the deletion.

9 Managing Build Nodes

■ Overview	156
■ The All Build Nodes Page	156
■ Adding a Build Node	158
■ Deleting a Build Node	158

Overview

Mobile Administrator allows you to connect to build nodes on Mac OS X and Windows 8.

A build node on	supports building apps for
Mac OS X	iOS and Android
Windows 8	Windows Phone and Windows RT


A build node is used if you have the source code (either stored locally or in a source code repository) and you want to remotely build the binaries for your apps.

A build node is not required if you already have the binaries or when you add an app from a vendor store. For example, you can do all development and build steps for an app with Mobile Designer, and you can then upload the ready-to-run binaries to Mobile Administrator to make the app available in the app store. Or you can just develop the source code with Mobile Designer and then let Mobile Administrator do the build.

Mobile Administrator provides continuous integration for mobile projects across all platforms. Builds run in the cloud without developers having to run the build environments for all platforms on their developer machines. Builds in the cloud can be scheduled when a source code repository has been defined in the build configuration of an app (see "[Scheduling a Build Job](#)" on page 162), and test runs can be organized to ensure the quality of the app (see "[Running Tests](#)" on page 162). Mobile Administrator can manage an arbitrary number of these build nodes in the cloud.

To manage the build nodes, you need the site-level permission **Manage Site**. See also "[Overview of Site-Level Permissions](#)" on page 141.

The All Build Nodes Page

When you click  and then **Build Nodes**, the **All Build Nodes** page is shown which lists all currently defined build nodes.

All Build Nodes							
Filter: <input type="text"/>							
	Owner	Available to All	Status	Node Version	Capabilities	Jobs Processed / Failed	Last Job At / Last seen
metaquark build node (10.16.30.13)	admin	<input checked="" type="checkbox"/>	ONLINE	9.7.0.0.220	Android 12, 13, 14, 15, 16, 17, 18, 19 iOS 6.1, 7.0 Mobile Designer 8.2.5.11.345, 8.2.6.2.353, 9.0.1.1.363, 9.5.1.0.375, 9.5.1.0.377, 9.6.0.0.381, 9.6.0.0.382, 9.6.0.0.384, 9.6.0.0.387, 9.6.1.0.390, 9.6.1.0.395, 9.7.0.0.398, 9.7.0.0.399	252 / 61	about 1 hour ago / Just now
Jonas's MacBook Pro (172.20.10.5)	jonas	<input checked="" type="checkbox"/>	OFFLINE	9.6.0.1.173	Android 16, 17, 18, 19 iOS 7.1 Mobile Designer 9.6.1.0.390, 9.6.1.0.392	5 / 0	7 months ago / 2 months ago

Tip: You can also access this page from the dashboard: In the **Domain Information** box, click the number that is shown next to **Build Nodes**.

Using this page, you can add new build nodes and delete existing build nodes. And you can click on a link in the **Owner** column to display the details of the user who has created the corresponding build node.

When the **Available to All** check box is selected, the build node is available to all users. When it is not selected, it is only available to the owner of the build node.

A build node can be online or offline. Offline means that the defined build node cannot be reached, for example, because the machine on which this build node runs has been switched off, or because the software for running the build node has not been started.

For each build node, the **Capabilities** column shows for which platforms and versions a build can be run. It also shows all Mobile Designer versions that are installed on the build node.

The **Jobs Processed / Failed** column includes the total number of build jobs for which an error has occurred during the build. To view the build jobs and their errors, go to the **All Build Jobs** page. See also ["Managing Build Jobs" on page 159](#).

Using the **Filter** box, you can restrict the list to show only those build nodes that meet your filter criteria. For example, you can display only the build nodes for a specific node version or only the build nodes that are currently online. See also ["Filtering Lists" on page 22](#).

Adding a Build Node


To add a build node, you have to download the file for the appropriate platform which is shown at the bottom of the **All Build Nodes** page. Each file allows you to install a wizard that is used to specify the required information for setting up the build node and connecting it to a Mobile Administrator instance. For detailed information, see ["Connecting Build Nodes" on page 36](#).

Deleting a Build Node

You can delete a build node, for example, if it has been offline for quite some time and is no longer used.

Note: All build jobs that still use the deleted build node will fail.

To delete a build node

1. Click  and then **Build Nodes**.
2. On the **All Build Node** page, select the check box for the build node that you want to delete and click **Delete**.

The build node will be deleted immediately. You will not be asked whether you are sure. However, this is not critical. As soon as the build node goes online again, an entry for this build node will reappear on the **All Build Node** page.

10 Managing Build Jobs

■ Overview	160
■ The All Build Jobs Page	160
■ Displaying the Details of a Build Job	161
■ Running Tests	162
■ Scheduling a Build Job	162
■ Relaunching a Build Job	162
■ Showing the Console Output for a Build Job	163
■ Showing the Errors for a Build Job	164
■ Deleting a Build Job	164

Overview

A build job runs on a build node and requires a build configuration. A build job is created when you launch a build configuration for an app. The outcome of a build job is a specific app version.


You can access the build jobs in two different ways:







- via the **Build Jobs** tab of an app (see ["Managing the Build Jobs of an App"](#) on page 97),
- via the list of all build jobs for all apps (see ["The All Build Jobs Page"](#) on page 160).

Build jobs are not required for apps that you pull from a vendor store.

To manage the build jobs, you need the site-level permission **Manage Build Jobs**. See also ["Overview of Site-Level Permissions"](#) on page 141.

The All Build Jobs Page

When you click  and then **Build Jobs**, the **All Build Jobs** page is shown which lists all build jobs which have ever been created (unless you delete them from this page).

All Build Jobs					
					Filter: <input type="text"/>
App	Build Configuration	Version	Status	Updated At	
 KarinDemo	iOS: KarinDemo iOS_Apple_Universal	0.0.2/2	SUCCESS	2014-09-03 12:46:17 CEST	
 MPConPreco	Android: MPConPreco AND_generic_Android3xAPI	0.0.7/6	SUCCESS	2014-08-28 16:17:27 CEST	
 MPConPreco	Android: MPConPreco AND_generic_Android4xAPI	0.0.7/6	SUCCESS	2014-08-28 16:16:26 CEST	

Tip: You can also access this page from the dashboard: In the **Domain Information** box, click the number that is shown next to **Build Jobs (Today)**.

Using this page, you can relaunch or delete build jobs, or display the details of a build job. When you display a build job, you can display the console output for the build job or any errors that may have occurred.

The status of a build job can be:

- **Initializing.** This is the first state after a build job has been launched: the source code for the app is created.

- **Pending.** This is the second state: the build job is ready to be processed and is waiting to be run.
- **Running.** This is the third state: the build job is running.
- **Success.** This is the last state: the build job has successfully created a new version of the associated app.
- **Error.** This is shown as the last state if the build job has failed.

The list can be sorted by clicking on a column header. For example, you can sort it by the **Updated At** date so that the latest updates are always shown at the top of the list.



Using the **Filter** box, you can restrict the list to show only those build jobs that meet your filter criteria. For example, you can display only the build jobs for a specific app. See also "[Filtering Lists](#)" on page 22.

Note: If you are looking for a specific build number, move the mouse over the different entries on the **All Build Jobs** page and check the URL that is shown in the status bar. The build number is shown at the end of the URL.

Displaying the Details of a Build Job

You can display a build job to view information such as the following: the build configuration that has been used, the user who has launched the build job, or the number of tests that have been run (these tests are defined in the source code). Several links are provided, for example, you can directly go to the corresponding app version or display the details of the user who launched the build job. Links are also provided for the input and output files so that you can view or download them.

To display the details of a build job

- To display the details via the list of all build jobs:
 1. Click  and then **Build Jobs**.
 2. On the **All Build Jobs** page, click the name of the build job that you want to display.
- To display the details via the app for which the build job has been created:
 1. Click  **Manage Apps**.
 2. On the **All Applications** page, click the app.
 3. Click **Build** on the left side.
 4. Click the **Build Jobs** tab.
 5. Click the name of the build job that you want to display.

Running Tests

If you want to run tests for an app, you have to enable the **Run tests after build** option in the build configuration of the app. All tests defined in the source code will then be run automatically after the build job has finished. You can also enable the **Require tests to pass** option to define that a build job can only receive the build status "Success" if all tests have run successfully. See also "[Adding a Build Configuration](#)" on page 91.

In the details of the resulting build job, you can then see how many tests have been run and whether they were successful or not.




Scheduling a Build Job

You can schedule automatic runs of a build configuration when the source code of an app is taken from a source code repository. To do so, you have to enable the **Scheduled?** option in the build configuration of the app. You can then define the time at which the app is to be built each day. You can also enable the **Enable commit trigger** option; the build is then started automatically each time a change is committed to the source code repository. See also "[Adding a Build Configuration](#)" on page 91.

Relaunching a Build Job

You can relaunch a build job, for example, if the first launch of the build configuration has resulted in the status "Error" and you have corrected these errors. This creates a new version of the associated app.

To relaunch a build job



1. Do one of the following:
 - To relaunch a build job via the list of all build jobs, click  and then **Build Jobs**.
 - To relaunch a build job via the app for which the build job has been created:
 - i. Click  **Manage Apps**.
 - ii. On the **All Applications** page, click the app.
 - iii. Click **Build** on the left side.
 - iv. Click the **Build Jobs** tab.
2. Do one of the following:
 - Click  for the build job that you want to relaunch.
 - Or click the name of the build job to display it and then click **Relaunch Build Job**.

The build status is now shown on the details page for the build job. The build job starts with the status "Pending" and then continues with the status "Running". When the build status "Success" is shown, the build job has successfully created a new version of the associated app.

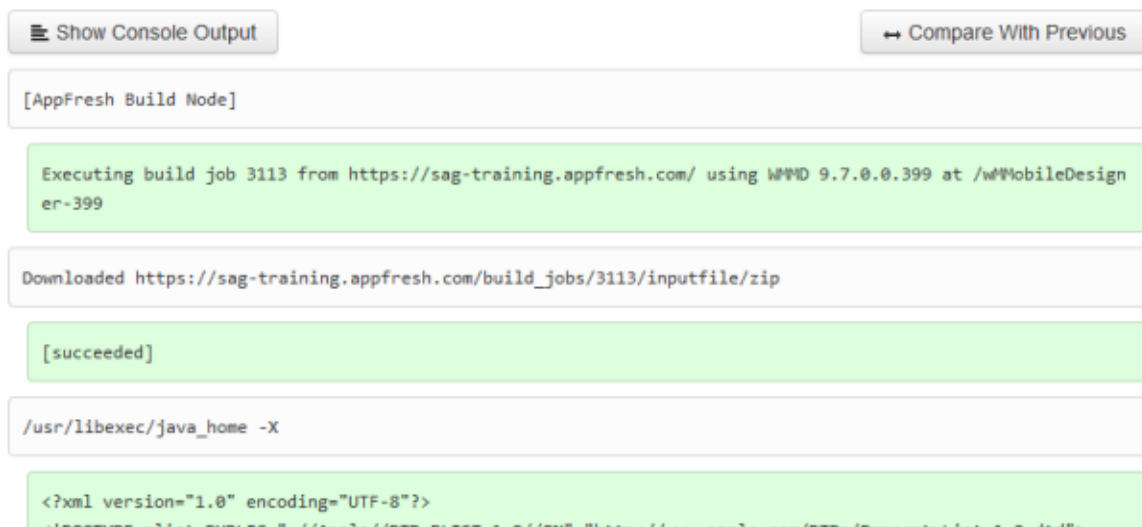
Showing the Console Output for a Build Job

You can display the console output for a build job. This is helpful when debugging an app.

To show the console output for a build job

- Do one of the following:
 - To show the console output via the list of all build jobs, click  and then **Build Jobs**.
 - To show the console output via the app for which the build job has been created:
 - Click  **Manage Apps**.
 - On the **All Applications** page, click the app.
 - Click **Build** on the left side.
 - Click the **Build Jobs** tab.
- Click the name of the build job to display it.
- Scroll down to the bottom of the page and click **Show Console Output**.

Information such as the following is shown:



```

Show Console Output Compare With Previous

[AppFresh Build Node]

Executing build job 3113 from https://sag-training.appfresh.com/ using WMD 9.7.0.0.399 at /w#MobileDesign
er-399

Downloaded https://sag-training.appfresh.com/build_jobs/3113/inputfile/zip

[succeeded]

/usr/libexec/java_home -X

<?xml version="1.0" encoding="UTF-8"?>
<DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">

```

- Click **Compare With Previous** if you want to compare the output with the log of the previous build job.



5. If you want to hide the console output, click **Show Console Output** once more.

Showing the Errors for a Build Job

When an error occurs during the build, a **Show Errors** button is shown in the details of the build job.

Note: A build job can receive the status "Success" even if one of the tests has failed. This depends on the setting of the **Require tests to pass** option in the build configuration. See also "[Adding a Build Configuration](#)" on page 91.

To show the errors for a build job

1. Do one of the following:
 - To show the errors via the list of all build jobs, click  and then **Build Jobs**.
 - To show the errors via the app for which the build job has been created:
 - i. Click  **Manage Apps**.
 - ii. On the **All Applications** page, click the app.
 - iii. Click **Build** on the left side.
 - iv. Click the **Build Jobs** tab.
2. Click the name of the build job to display it.
3. Scroll down to the bottom of the page and click **Show Errors**.


Note: This button is only shown if an error has occurred during the build.


4. Click **Compare With Previous Errors** if you want to compare the errors for the current build with the errors for the previous build.
5. If you want to hide the errors, click **Show Errors** once more.

Deleting a Build Job

You can delete old build jobs in which you are no longer interested. Keep in mind that this also deletes all console output and error logs for these build jobs.

To delete a build job

1. Do one of the following:
 - To delete a build job via the list of all build jobs:
 - i. Click  and then **Build Jobs**.

- ii. Select the check box for the build job that you want to delete and click **Delete**.
- To delete a build job via the app for which the build job has been created:
 - i. Click  **Manage Apps**.
 - ii. On the **All Applications** page, click the app.
 - iii. Click **Build** on the left side.
 - iv. Click the **Build Jobs** tab.
 - v. Select the check box for the build job that you want to delete and click **Delete Selected**.

You can also click the name of the build job to display it and then click **Delete Build Job**.

A dialog box appears, asking whether you are sure.

2. Click **OK** to confirm the deletion.

11 Managing Product Stages

■ Overview	168
■ The All Product Stages Page	168
■ Adding a Product Stage	168
■ Deleting a Product Stage	169


Overview


You assign a product stage to an app when you add a new app version or when you edit a specific version of the app. As a rule, your users can only see the app versions in your app store for which the product stage "stable" has been defined. This corresponds to the application-level permission **View and Download Stable Versions**. During the development of your app, however, it may be helpful to test unstable versions of your app. You can then grant the application-level permission **Download Unstable Versions** to your developers so that they can view and download unstable versions from the app store.

By default, Mobile Administrator is delivered with two product stages: a stable product stage with the name "Production" and an unstable product stage with the name "Unstable". You can also define additional product stages, for example, for the different lifecycle stages of your apps such as development or test, where each stage can be defined either as stable or unstable. Or you may want to define both an unstable development stage and a stable development stage.

To manage the product stages, you need the site-level permission **Manage Site**. See also ["Overview of Site-Level Permissions" on page 141](#).

The All Product Stages Page

When you click  and then **Product Stages**, the **All Product Stages** page is shown which lists all currently defined product stages. For each stage, the number of app versions in this stage is shown. The type of a product stage can be "Stable" or "Unstable".



All Product Stages		
Name	Type	Associated Versions
<input type="checkbox"/> Production	stable	76
<input type="checkbox"/> Unstable	unstable	77
<input type="checkbox"/> Prerelease	unstable	22
<input type="checkbox"/>  Delete		

Using this page, you can add new product stages, delete product stages, or display and edit the details of a product stage.

Adding a Product Stage

When you add a product stage, you can define it as either stable or unstable.


To add a product stage

1. Click  and then **Product Stages**.
2. On the **All Product Stages** page, click  .
3. On the resulting page, specify a name for the product stage.
4. Do one of the following:
 - Click the **Stable** check box if you want to create a product stage of type "Stable".
 - Leave the check box empty if you want to create a product stage of type "Unstable".
5. Click **Create Product Stage**.

Deleting a Product Stage

When you delete a product stage, its definition will also be removed from all app versions for which this stage has been defined.

To delete a product stage

1. Click  and then **Product Stages**.
2. On the **All Product Stages** page, do one of the following:
 - Select the check box for the product stage that you want to delete and click **Delete**.
 - Or click the name of the product stage to display it and then click **Delete Product Stage**.

A dialog box appears, asking whether you are sure.

3. Click **OK** to confirm the deletion.

12 Managing Developer Certificates

■ Overview	172
■ The All Certificates Page	172
■ Deleting a Certificate	173

Overview


Certificates are required for building the apps for the different platforms. You obtain them, for example, when you enroll in Apple's iOS Developer Program, and to have to upload them to Mobile Administrator. See the following configuration topics for more detailed information:

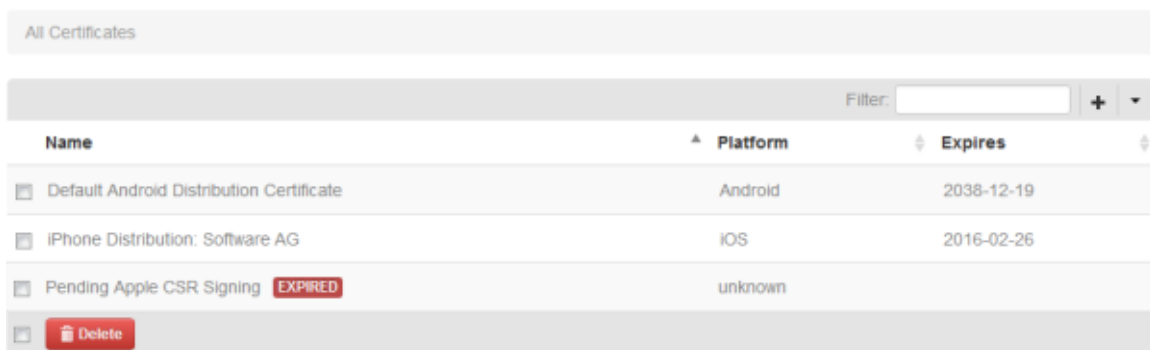
- ["Adding Code Signing Certificates for iOS" on page 32](#)
- ["Adding Code Signing Certificates for Android" on page 34](#)
- ["Adding Code Signing Certificates for Windows Phone" on page 34](#)
- ["Adding Code Signing Certificates for Windows 8/RT" on page 35](#)

Especially in large enterprises, where mobile applications are developed by multiple teams or external agencies, having your enterprise certificates managed by Mobile Administrator allows for a fine-grained configuration of who can deploy your mobile applications. Without Mobile Administrator, the enterprise certificates need to be shared with everyone who needs to perform deployment. With Mobile Administrator, enterprise certificates are managed centrally without giving direct access to the certificates to everyone.

To manage the developer certificates, you need the site-level permission **Manage Site**. See also ["Overview of Site-Level Permissions" on page 141](#).



The All Certificates Page

When you click  and then **Developer Certificates**, the **All Certificates** page is shown which lists all currently defined certificates, together with their expiration dates. This page also shows all certificates for which the final upload is still pending. When a certificate has expired or is about to expire, the information "Expired" or "Expires soon" is shown next to the certificate name.



Name	Platform	Expires
Default Android Distribution Certificate	Android	2038-12-19
iPhone Distribution: Software AG	iOS	2016-02-26
Pending Apple CSR Signing EXPIRED	unknown	

Using this page, you can upload new certificates and delete existing certificates. This comprises the following:

- **Developer certificates** for Android and Windows (uploaded via ) , and
- **iOS distribution certificates** (generated and uploaded via the  menu).

For detailed information on how to upload the different types of certificates, see the information on adding code signing certificates for the different platforms in ["Configuring Mobile Administrator" on page 27](#).


When you click a certificate name to display it, you can see in which build configurations the certificate is used. You can then click a build configuration to display information on the app for which the build configuration has been created. For an iOS certificate, you can also see the associated provisioning profiles and when they expire. An exception is an entry for which "Pending" is shown in the **Name** column. When you click such an entry, you can proceed with the signing process for an iOS developer certificate.

Using the **Filter** box, you can restrict the list to show only those certificates that meet your filter criteria. For example, you can display only the "expired" or "pending" certificates. See also ["Filtering Lists" on page 22](#).

Deleting a Certificate

You can delete a certificate, for example, if it has expired and is no longer used.

To delete a certificate

1. Click  and then **Developer Certificates**.
2. On the **All Certificates** page, do one of the following:
 - Select the check box for each certificate that you want to delete and click **Delete**.
 - Or, if you only want to delete a single certificate, click the name of the certificate to display it and then click **Delete Certificate**.

A dialog box appears, asking whether you are sure.

3. Click **OK** to confirm the deletion.

13 Managing Provisioning Profiles


■ Overview	176
■ The All iOS Provisioning Profiles Page	176
■ Deleting a Provisioning Profile	176

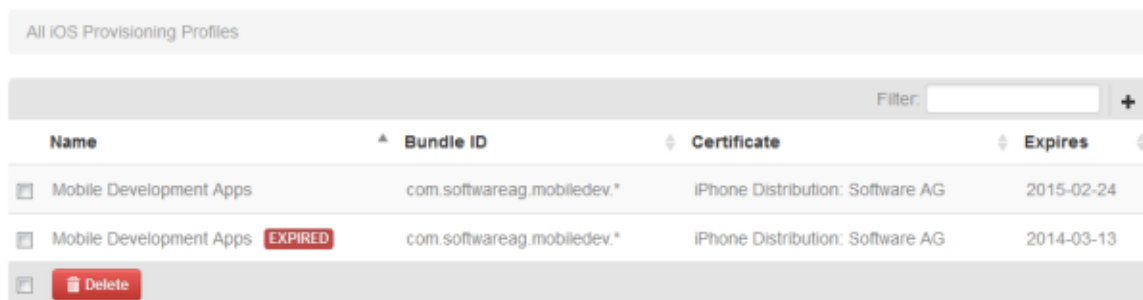
Overview

Provisioning profiles are used to build apps for iOS. You obtain them when you enroll in Apple's iOS Developer Program, and to have to upload them to Mobile Administrator. See ["Adding Code Signing Certificates for iOS" on page 32](#) for more detailed information.

To manage the provisioning profiles, you need the site-level permission **Manage Site**. See also ["Overview of Site-Level Permissions" on page 141](#).

The All iOS Provisioning Profiles Page

When you click  and then **Provisioning Profiles**, the **All iOS Provisioning Profiles** page is shown which lists all currently defined provisioning profiles, together with their expiration dates. When a profile has expired or is about to expire, the information "Expired" or "Expires soon" is shown next to the profile name.



Name	Bundle ID	Certificate	Expires
Mobile Development Apps	com.softwareag.mobiledev.*	iPhone Distribution: Software AG	2015-02-24
Mobile Development Apps EXPIRED	com.softwareag.mobiledev.*	iPhone Distribution: Software AG	2014-03-13

Using this page, you can upload new provisioning profiles and delete existing provisioning profiles. For detailed information on how to upload a provisioning profile, see ["Uploading an iOS Provisioning Profile" on page 33](#).


When you click a provisioning profile to display it, you can see the name of the certificate which matches this provisioning profile, and you can see in which build configurations the provisioning profile is used. You can then click a build configuration to display information on the app for which the build configuration has been created.

Using the **Filter** box, you can restrict the list to show only those provisioning profiles that meet your filter criteria. For example, you can enter "expired" to display only the expired profiles. See also ["Filtering Lists" on page 22](#).

Deleting a Provisioning Profile

You can delete a provisioning profile, for example, if it has expired and is no longer used.

To delete a provisioning profile

1. Click  and then **Provisioning Profiles**.
2. On the **All iOS Provisioning Profiles** page, do one of the following:
 - Select the check box for each provisioning profile that you want to delete and click **Delete**.
 - Or, if you only want to delete a single provisioning profile, click the name of the provisioning profile to display it and then click **Delete Provisioning Profile**.

A dialog box appears, asking whether you are sure.

3. Click **OK** to confirm the deletion.

14 Re-Signing Applications


■ Overview	180
■ The Application Re-sign Page	180
■ Re-signing an iOS App	181
■ Re-signing an Android App	181
■ Re-signing a Windows Phone App	182
■ Re-signing a Windows 8/RT App	182
■ Deleting a Re-signing Job	183

Overview

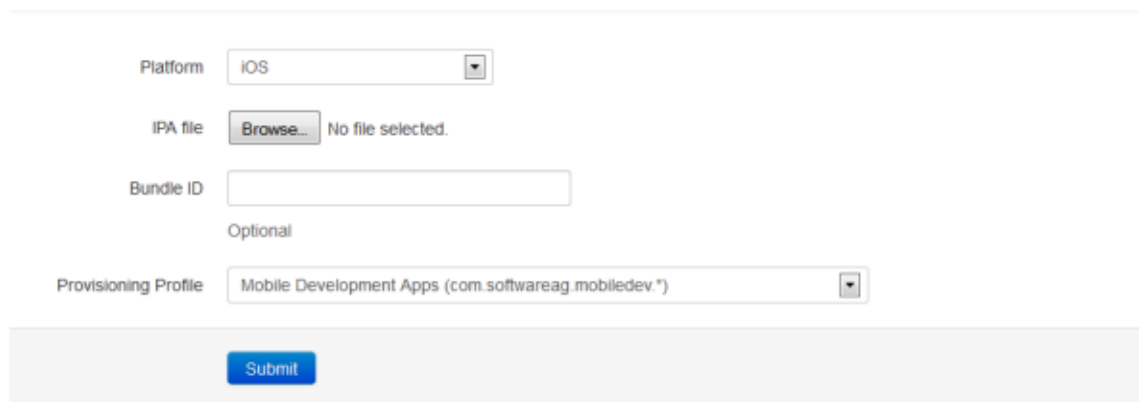
When the developer certificate (Android and Windows) or provisioning profile (iOS) for an app has expired, you can upload a new valid developer certificate or provisioning profile. After that, you can upload and re-sign an app with the new certificate or profile without having to rebuild the app.

To re-sign apps, you need the site-level permission **Manage Site**. See also "[Overview of Site-Level Permissions](#)" on page 141.

The Application Re-sign Page

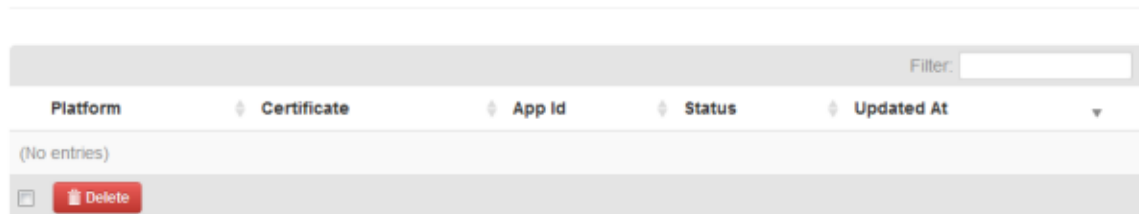
When you click  and then **Application Re-sign**, a page is shown which allows you to upload and resign an app with the selected developer certificate or provisioning profile. The options that are shown at the top of the page depend on the selected platform.

Application Re-sign



The screenshot shows the 'Application Re-sign' form. It includes a 'Platform' dropdown menu set to 'iOS'. Below it is an 'IPA file' section with a 'Browse...' button and the text 'No file selected.'. There is a 'Bundle ID' text input field. Below that is an 'Optional' section with a 'Provisioning Profile' dropdown menu set to 'Mobile Development Apps (com.softwareag.mobiledev.*)'. At the bottom of the form is a blue 'Submit' button.

Re-signing Jobs



The screenshot shows the 'Re-signing Jobs' table. It has a 'Filter' input field at the top right. The table has columns: 'Platform', 'Certificate', 'App Id', 'Status', and 'Updated At'. Below the columns, it says '(No entries)'. At the bottom of the table, there is a red 'Delete' button.


Platform	Certificate	App Id	Status	Updated At
(No entries)				

For each re-signed app, a re-signing job is shown at the bottom of the page. Such a job provides the same status information as a build job (with the exception that a build is not necessary for the re-sign). You can click the entry for a re-sign job to display more information. This is helpful, for example, if job remains in the "Pending" status for quite some time and you want to find out the reason for this. One possible reason may be that the build node which supports the defined platform is currently not online.

Re-signing an iOS App

Use the following procedure after you have uploaded a new valid provisioning profile. See also "[Uploading an iOS Provisioning Profile](#)" on page 33.

To re-sign an iOS app

1. Click  and then **Application Re-sign**.
2. From the **Platform** drop-down list box, select **iOS**.
3. Specify the following options:


Option	Description
IPA file	Click Browse and then upload the app that you want to re-sign.
Bundle ID	Optional. Specify a new bundle ID if you want to change the bundle ID of the app.
Provisioning profile	Select the provisioning profile to be used. The drop-down list box provides for selection all provisioning profiles which have been uploaded.

4. Click **Submit**.

Re-signing an Android App

Use the following procedure after you have uploaded a new valid developer certificate. See also "[Uploading a Developer Certificate for Android](#)" on page 34.

To re-sign an Android app

1. Click  and then **Application Re-sign**.
2. From the **Platform** drop-down list box, select **Android**.
3. Specify the following options:

Option	Description
APK file	Click Browse and then upload the app that you want to re-sign.


Option	Description
Certificate	Select the certificate to be used. The drop-down list box provides for selection all Android certificates which have been uploaded.

- Click **Submit**.

Re-signing a Windows Phone App

Use the following procedure after you have uploaded a new valid developer certificate. See also "[Uploading a Developer Certificate for Windows Phone](#)" on page 35.

To re-sign a Windows Phone app

- Click  and then **Application Re-sign**.
- From the **Platform** drop-down list box, select **Windows Phone**.
- Specify the following options:

Option	Description
XAP file	Click Browse and then upload the app that you want to re-sign.
Application ID	Optional. Specify a new application ID if you want to change the application ID of the app.
Certificate	Select the certificate to be used. The drop-down list box provides for selection all Windows Phone certificates which have been uploaded.

- Click **Submit**.

Re-signing a Windows 8/RT App

Use the following procedure after you have uploaded a new valid developer certificate. See also "[Uploading a Developer Certificate for Windows 8/RT](#)" on page 35.

To re-sign a Windows 8/RT app

- Click  and then **Application Re-sign**.

- From the **Platform** drop-down list box, select **Windows 8/RT**.
- Specify the following options:


<u>Option</u>	<u>Description</u>
APPX file	Click Browse and then upload the app that you want to resign.
Application ID	Optional. Specify a new application ID if you want to change the application ID of the app.
Certificate	Select the certificate to be used. The drop-down list box provides for selection all Windows 8 and Windows RT certificates which have been uploaded.

- Click **Submit**.

Deleting a Re-signing Job

You can delete old re-signing jobs in which you are no longer interested.

To delete a re-signing job

- Click  and then **Application Re-sign**.
- On the resulting page, do one of the following:
 - Select the check box for each re-signing job that you want to delete and click **Delete**.
 - Or, if you only want to delete a single re-signing job, click the name of the job to display it and then click **Remove Build Job**.

A dialog box appears, asking whether you are sure.

- Click **OK** to confirm the deletion.

15 Sales and Trends on iTunes Connect


■ Overview	186
■ The All iTunes Connect Vendors Page	186
■ Adding a New iTunes Connect Vendor	186
■ Editing the Vendor Information	187
■ Downloading Reports From iTunes Connect Manually	187
■ Adding Reports to Mobile Administrator Manually	187
■ Exporting Reports to Your File System	188
■ Deleting All Reports	188
■ Deleting a Vendor	188

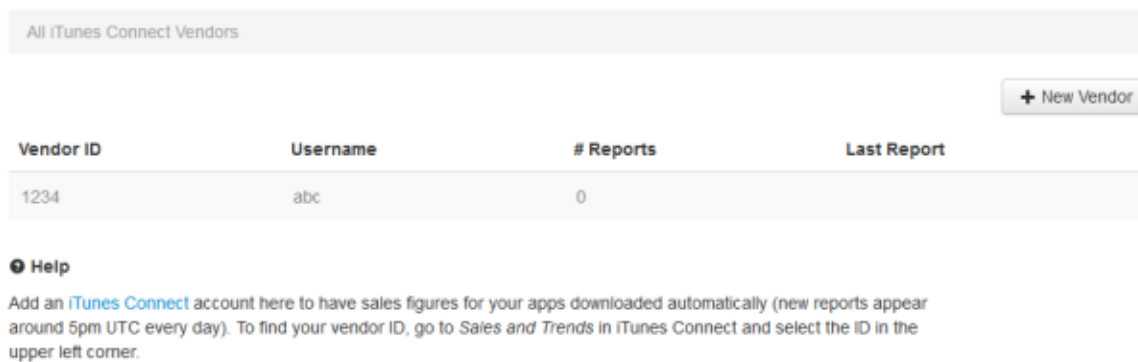
Overview

If you want to use this feature, you need an iTunes Connect account and a vendor ID. You can then automatically download the Sales and Trends reports for your apps into Mobile Administrator. New reports appear in iTunes Connect around 5:00 pm UTC every day. See the iTunes Connect documentation for detailed information on the Sales and Trends reports.

To use this feature, you need the site-level permission **Manage Site**. See also "[Overview of Site-Level Permissions](#)" on page 141.

The All iTunes Connect Vendors Page


When you click  and then **iTunes Connect**, a page is shown which allows you to add a new vendor for each iTunes Connect account you have. A link to the iTunes Connect website is provided in case you want to sign in. If vendors have already been defined, they are shown on this page.



All iTunes Connect Vendors

[+ New Vendor](#)

Vendor ID	Username	# Reports	Last Report
1234	abc	0	

 **Help**


Add an [iTunes Connect](#) account here to have sales figures for your apps downloaded automatically (new reports appear around 5pm UTC every day). To find your vendor ID, go to *Sales and Trends* in iTunes Connect and select the ID in the upper left corner.

When you click a vendor to display the vendor details, you can see a list of automatically downloaded reports. You can also manually download the reports. Each report is a CSV file.

Adding a New iTunes Connect Vendor

When you add a vendor, you have to specify a vendor ID. To find your vendor ID, sign in to your iTunes Connect account, go to **Sales and Trends**, and select **Top Content > Reports** in the upper left corner. Your vendor ID is then shown and you can write it down.

To add a new iTunes Connect vendor

1. Click  and then **iTunes Connect**.
2. Click **New Vendor**.


3. Specify your vendor ID, and your iTunes Connect user name and password.
4. Click **Create iTunes Connect Vendor**.

When valid vendor information has been specified, the reports are immediately downloaded.

Editing the Vendor Information

You can edit the information that you have specified for your iTunes Connect account, for example, if you have changed the password for this account.


To edit the vendor information

1. Click  and then **iTunes Connect**.
2. Click the vendor to display the details for that vendor.
3. Click **Edit Vendor**.
4. Change the required information (vendor ID, iTunes Connect user name and/or password).
5. Click **Update iTunes Connect Vendor**.

Downloading Reports From iTunes Connect Manually

If you do not want to wait until the next reports will automatically be downloaded into Mobile Administrator, you can download them manually.


To download reports manually

1. Click  and then **iTunes Connect**.
2. Click the vendor to display the details for that vendor.
3. Click **Download Reports Now**.

Adding Reports to Mobile Administrator Manually

You can manually add reports to Mobile Administrator that you have directly downloaded from iTunes Connect (without the use of Mobile Administrator). To do so, you have to upload the zip file containing these reports from your file system.

To add reports manually


1. Click  and then **iTunes Connect**.
2. Click the vendor to display the details for that vendor.

3. Click **Browse** and then select the zip file.
4. Click **Add Reports** to upload the zip file.

Exporting Reports to Your File System

If you want to display the contents of the reports, you first have to export them to your file system. All reports that are currently listed on the details page are then downloaded as a zip file.


To export the reports

1. Click  and then **iTunes Connect**.
2. Click the vendor to display the details for that vendor.
3. Click **Export Zip**.

Deleting All Reports

If all of the reports that are listed in the vendor details are no longer needed, you can delete them.


To delete all reports

1. Click  and then **iTunes Connect**.
2. Click the vendor to display the details for that vendor.
3. Click **Delete All Reports**.

Deleting a Vendor

If a vendor is no longer needed, you can delete the corresponding entry from Mobile Administrator.

To delete a vendor

1. Click  and then **iTunes Connect**.
2. Click the vendor to display the details for that vendor.
3. Click **Delete Vendor**.

A dialog box appears, asking whether you are sure.

4. Click **OK** to confirm the deletion.

16 Maintaining Mobile Administrator


■ Overview	190
■ The Maintenance Page	190

Overview

Mobile Administrator allows you to view a number of log files and processes. It also offers a number of cleanup tasks for fixing common issues in the database. These maintenance functions pertain to the domain in which you are currently logged in.

If you want to use the maintenance functions, you need the site-level permission **Manage All Sites**. See also "[Overview of Site-Level Permissions](#)" on page 141.

The Maintenance Page

When you click  and then **Maintenance**, the **Maintenance** page is shown providing several tabs. See the following topics for more information:

- ["Domain Log" on page 190](#)
- ["Server Logs" on page 191](#)
- ["Cleanup Tasks" on page 191](#)
- ["Process Info" on page 192](#)

Domain Log

The **Domain Log** tab provides several pages with information on the following actions:

Action	Description
Login	Occurs when a user logs in to Mobile Administrator. This also includes the mobile web site and the app store client.
Logout	Occurs when a user logs out from Mobile Administrator. This also includes the mobile web site and the app store client.
Create	Occurs when an object is created.
Update	Occurs when an object is updated.
Destroy	Occurs when an object is deleted.

For each action, a timestamp is shown and the affected object. An object is anything that can be changed with Mobile Administrator, for example, a build node, build job, product (app) version, user, device, certificate, authentication token, or policy. If applicable, a user name and the changed attributes are also shown.

You can click the entry for an action to display more information. Links on the resulting page allow you to get more information, for example, you can display the user details, or you can display a device and then manage it.

Note: If you only want to see the log entries for a specific app, see ["Viewing the Log Information for an App"](#) on page 67.

Server Logs

The **Server Logs** tab allows you to view and download different types of server logs. This is helpful when debugging API requests and general server functionality. The following log files are available:

Log File	Description
apache_access.log	Access log of the web server.
apache_error.log	Error log of the web server.
ldapservice.log	Error log of the LDAP service. You should view this log if you have problems with the LDAP connection.
ldapservice.request.log	Request log of the LDAP service.
production.log	Main log file of the application server.
production_warn.log	Log file containing only the warnings and errors of the application server.
scheduler.log	Log file containing the scheduled tasks.
web-1.log	Log file of the application server process.
worker-1.log	Log file for the Rails worker process.

To display the contents of a log file, select its name in the drop-down list box and then click **Show**. If you want to download the log file that is currently shown, click the **Download *file-name*** button.

Cleanup Tasks

The **Cleanup Tasks** tab provides a number of tasks for fixing common issues in the database. The following buttons are available:

Button	Description
Sanitize DB	Cleans up various known issues in the database structure. These can be, for example, problems when displaying or downloading apps.
Update Device Models	Updates the list of device models in the database to the latest information that is shipped with this version of Mobile Administrator. This is helpful if you have updated Mobile Administrator.
Create Default Objects	Creates the following default objects in the current domain: administration user, "All Users" group, default Android certificate, smart categories and product stages. This is helpful if you have deleted a default object and you want to have it back.
Reset Binary Compatibility	Resets the compatibility information for all binaries and device models and recreates them. This can take a while.

When you click one of the above buttons, a message is shown indicating that the task has been started.

Process Info

The **Process Info** tab lists the processes related to Mobile Administrator. You can view this tab to make sure that these processes are operating correctly. The status of a process can be one of the following:

- **Running.** The process operates correctly.
- **Not running.** An error has occurred. Inform your system administrator.

17 Using the App Store on a Mobile Device

■ Overview	194
■ Using the App Store Client on a Mobile Device	194
■ Using the App Store Website on a Mobile Device	199

Overview

The end users can download onto their mobile devices the apps that you have made available in your app store. They can do this in two different ways:

- **App store client.** The app which makes up your app store (also called the "app store client") is installed on the mobile device. The app store client can be installed by the users their own devices, or it can be pre-installed by IT on company-managed devices. Using the app store client, the users can download the required apps onto their mobile devices.

When a network connection is not available, the users can nevertheless work offline with the downloaded apps. The data will be stored locally within the app and will be synchronized with the server when the network connection is restored.

- **App store website.** The users can access the mobile site of your app store using the browser on the mobile device. They can then download the apps from the web site.

In both cases, each user first has to use the browser on the mobile device to access the login page of your app store. The user can then choose whether to download the app (the app store client) or to log in to the website. The administrator normally informs the authorized users about the required URL.

Important: Software AG recommends installing the app store client.

Using the App Store Client on a Mobile Device

The app store client on a mobile device offers for download the apps which have been developed for the operating system that is running on the current device. For example, if an app has only been build to run on iOS, it will only be shown on iOS devices. It will not be shown on Android or Windows Phone devices.

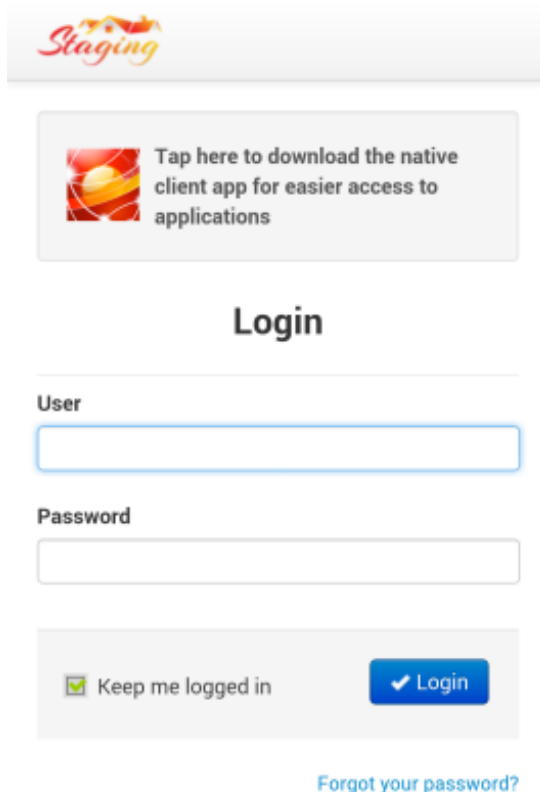
Installing the App Store Client

When you install the app store client on your device, it may happen that specific settings from your device are used. For example, button names, menu names and options may be shown in German.

To install the app store client

1. Android only: Go to **Settings** and enable the security option to install from unknown sources.
2. Use the browser on your mobile device to connect to the web site of your app store. Enter the URL that you have received from your administrator.

A page such as the following is shown in the browser.



Staging

Tap here to download the native client app for easier access to applications

Login

User

Password

Keep me logged in

[Forgot your password?](#)

3. Windows only: The page from which you can download the app store client provides a link for installing the company enrollment token. Install this token so that you can download and install the app store client.
4. Tap on the **Tap here ...** area to download the app store client.

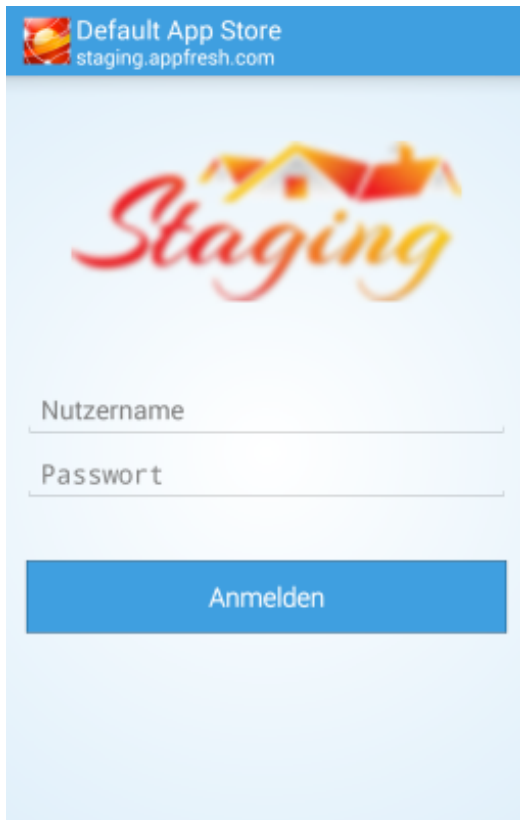
Note: To download the app, you need not enter your user name and password on this page. This is only required if you want to log in to the mobile version of the app store.

5. Proceed as follows, depending on the operating system that is running on your device.
 - iOS and Windows: Confirm that you want to install the app.
 - Android: Find the downloaded .apk file and tap on it to start the installation.

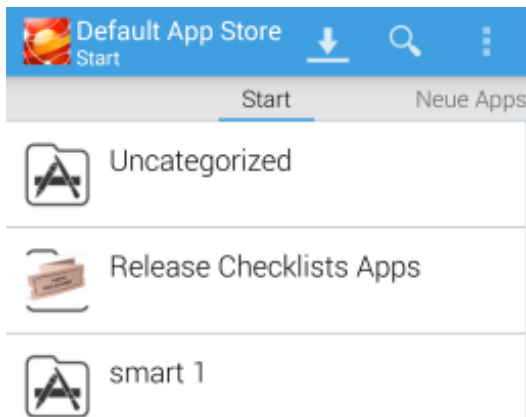
Using the App Store Client

When you invoke the app store client for the first time, you have to log in using your user name and password.


If the language of your device is German, the app store client will also use the German language. In all other cases, the app store is shown in English.



The start page of the app store client shows the defined categories.

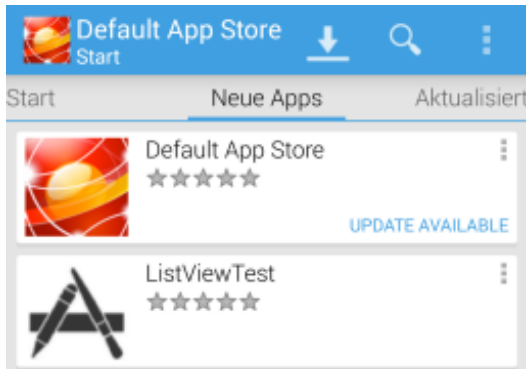


When you tap on a category, the apps that have been assigned to this category are shown. You can then display and download the apps. As a rule, you will only see the app versions for which the product stage "stable" has been defined. With the appropriate permission, however, you will also be able to see "unstable" app versions.


If you know the name of an app or a part of the app name, you can click  to locate that app without having to search the categories.

When you swipe the start page to the left, new and updated apps in the app store are shown. When an app is already installed on your device, "Installed" is shown for that

app. If a newer version can be downloaded for an installed app, "Update available" is shown for that app. When you tap on an app, you can display and download/update the app. The list of new apps only shows a limited number of apps, sorted by age. If you want to see all apps, you have to display them via the above-mentioned categories.



When you swipe the start page one more time to the left, any apps are shown that have been updated in the app store (for example, via a new build job).

You can click  to display a list with the apps that you have downloaded. Using the wastebasket icon on that page, you can delete the list.

Allowing the Mobile Device Management

When the app store client has been installed on a mobile device, the user has the possibility to allow the mobile device management (MDM). When this has been allowed, the administrator and the user who owns the device can remotely manage the device. This is helpful, for example, when a device is lost or stolen. It is then possible to lock or wipe the device.

Note: An administrator can also install and update selected apps directly on specific devices over the air, and can also remove them from these devices. See also ["Managing the Devices on Which the App Can be Installed" on page 100.](#)


To allow the mobile device management

1. In the app store client, go to **Settings**.
2. Check **Allow Device Management**.

Remotely Locking or Wiping a Mobile Device

If a device is lost or stolen, you have the possibility to remotely lock or wipe the device using Mobile Administrator on the PC. The prerequisite for this is that mobile device management (MDM) has been allowed on the device, in the app store client. The device can then be managed by the administrator and by the user who owns the device.

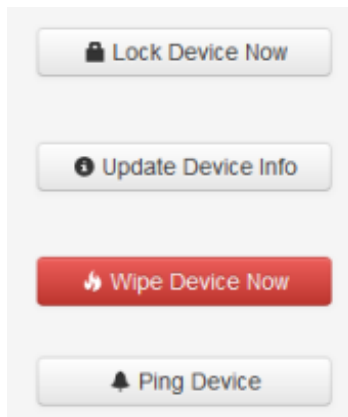
To remotely lock or wipe a mobile device

1. Log in to Mobile Administrator on the PC.
2. Click  **Devices**.

An administrator can see the devices of all users. An end user can only see the own devices.

3. Click the link for the device that you want to lock or wipe.

If the device management has been allowed on the mobile device, the following commands are shown on the **Device** tab of the resulting page.



4. Click the button for the command that you want to execute on the device. For more information, see ["Managing a Device" on page 114](#).

Removing the Mobile Device Management

You can disable the mobile device management directly on the mobile device, in the app store client. This will remove any of your organization-specific policies, certificates, email accounts and apps while leaving the rest of the device as-is.

Note: Mobile device management is not supported for Windows Phone.

To remove the mobile device management

- On an Android device, proceed as follows:
 1. In the app store client, go to **Settings**.
 2. Uncheck **Allow Device Management**.
- On an iOS device, proceed as follows:
 1. Go to **Device Settings**.
 2. Go to **General > Device Management**.
 3. Tap **Profile**.

4. Tap **Remove Management**.

Using the App Store Website on a Mobile Device

As in the app store client, the mobile site in the browser offers for download the apps which have been developed for the operating system that is running on a device.

Accessing the App Store in the Browser

To view the contents of your app store in the browser, you have to log in using your user name and password.

To access the app store in the browser

1. Use the browser on your device to connect to the web site of your app store. Enter the URL that you have received from your administrator.
2. Enter your user name and password and click **Login**.

Using the App Store in the Browser

When you access the app store via the browser of the mobile device, similar information is shown as on the **App Store** page that you can see in Mobile Administrator: the available apps are shown sorted by categories.

As a rule, you will only see the app versions for which the product stage "stable" has been defined. With the appropriate permission, however, you will also be able to see "unstable" app versions.

When you display an app, a **Download** button is provided.

If you have administrator rights, an additional button **Manage Apps** is provided further down on the page. When you tap this button, the same information is shown as on the **App Details** page on the PC and it is possible, for example, to export, share or delete the app. See also "[Managing the App Details](#)" on page 63.

If you want to log out, scroll down to the bottom of the page and tap the **Logout** link that is shown there.

18 Frequently-Asked Questions

■ App Management	202
■ Device Management	202
■ Certificate Management	203

App Management

How can I ensure that only specific developers can see and test unstable versions in the app store?

Grant the **Download Unstable Versions** permission to these users. You can do this on the **Permissions** page of the app. See also ["Managing the Permissions of an App" on page 83](#).

How can I ensure that an app can only be used by certain users?

Use the permissions functionality on the **Permissions** page of the app. See also ["Managing the Permissions of an App" on page 83](#).

How can I respond to a user comment?

There is no response capability yet. You can add another comment, which may be seen as a response to the previous comment.

Device Management

How can I register devices and assign them to users?

With the "Choose Your Own Device" (CYOD) concept, you have a number of devices that are owned by your company which you give out to selected users. The device is automatically registered when the user logs in to the app store client with that device.

How can I ensure that my apps can only be installed on devices on which MDM has been allowed?

Edit the app details and set the **Available on managed devices only** option. See also ["Editing an App" on page 65](#).

How can I update the installed apps over the air?

This is only possible on managed devices, that is, on devices where the mobile device management (MDM) has been allowed in the app store client. If you have a new version of an app that you want to make available on all devices on which it has been installed, go to the **Devices** page of that app, select all users by clicking the corresponding check box below the list of users, and click **Update**. See also ["Managing the Devices on Which the App Can be Installed" on page 100](#).

Is the mobile device management still active on a device after the app store client has been deleted from that device?

On iOS: yes. On Android: no.

Can an administrator remotely allow MDM for a device?

No, the mobile device management (MDM) can only be allowed directly on the device.

Which types of emails/notifications can be sent and how do I define them?

Email notifications are sent for expiring certificates (see below), when build jobs are completed (this needs to be defined in the build configuration, see ["Editing a Build Configuration" on page 96](#)) and when the export of an app has finished (see also ["Exporting an App" on page 66](#)).

Certificate Management

How can I be informed when a certificate is about to expire or has already expired?

Developer certificates and iOS provisioning profiles: you will automatically receive an email 14 days before the expiration date if you are either a domain administrator (see the **Admin email** option in ["Editing the Domain" on page 133](#)) or the owner of an app which uses this certificate or profile in one of its build configurations.

MDM certificates and CA certificates: no notifications are sent yet.